Shielding Europe with the Common Security and Defence Policy

The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment

Studies of the Central European Professors' Network
ISSN 2786-2518

Shielding Europe with the Common Security and Defence Policy

The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment

Edited by

Katarzyna Zombory

János Ede Szilágyi

On the occasion of the Hungarian Presidency of the Council of the European Union

CEA PUBLISHING

MISKOLC – BUDAPEST | 2024

STUDIES OF THE CENTRAL EUROPEAN PROFESSORS' NETWORK

Shielding Europe with the Common Security and Defence Policy
The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment

ISBN 978-615-6474-63-6 (printed version)
ISBN 978-615-6474-64-3 (pdf)
ISBN 978-615-6474-65-0 (epub)

https://doi.org/10.54237/profnet.2024.zkjeszcodef

The topic of this monograph was chosen by the Central European Academy with regard to the themes of the Hungarian Presidency of the Council of the European Union in 2024. The Central European Academy has published this monograph in honour of the Hungarian Presidency. The views expressed in this monograph reflect the views of the authors and not those of the Hungarian government.

Published by
Central European Academic Publishing
(Miskolc, Hungary)
1122 Budapest, Városmajor St. 12 (Hungary)

Design, layout, ebook
IDEA PLUS (Elemér *Könczey*, Botond *Fazakas*)
Kolozsvár / Cluj-Napoca (Romania)

Studies of the Central European Professors' Network
ISSN 2786-2518

Description

The book series *Studies of the Central European Professors' Network* publishes the results of research by members of the Central European Professors' Network established by the Budapest-based Ferenc Mádl Institute of Comparative Law in 2021. Since 2022, the Network is operated by the Central European Academy of the University of Miskolc.

The primary aim of the series is to present and address legal issues that are strongly related to the Central European region, taking into account the particular legal traditions, culture, and approach of the countries therein. The authenticity of the books can be seen in the fact that renowned authors from the Central European region write about the legal instruments of countries of the Central European region in English. The book series aims to establish itself as a comparative legal research forum by contributing to the stronger cooperation of the countries concerned and by ensuring the "best practices" and making different legal solutions available and interpretable to all of the states in Central Europe. However, it also aims to provide insights and detailed analyses of these topics to all interested legal scholars and legal practitioners outside the region so that they might become acquainted with the legal systems of Central European countries regarding a great variety of subjects.

Other titles in the book series *Studies of the Central European Professors' Network*

2021

Tímea *Barzó* – Barnabás *Lenkovics* (eds.): *Family Protection From a Legal Perspective*

Zoltán *J. Tóth* (ed.): *Constitutional Reasoning and Constitutional Interpretation*

Paweł *Sobczyk* (ed.): *Religious Symbols in the Public Sphere*

Marcin *Wielec* (ed.): *The Impact of Digital Platforms and Social Media on the Freedom of Expression and Pluralism*

2022

Paweł *Sobczyk* (ed.): *Content of the Right to Parental Responsibility: Experiences – Analyses – Postulates*

Zoltán *J. Tóth* (ed.): *Constitutional and Legal Protection of State and National Symbols in Central Europe*

János Ede *Szilágyi* (ed.): *Constitutional Protection of the Environment and Future Generations: Legislation and Practice in Certain Central European Countries*

2023

Marcin *Wielec* (ed.): *The Right to Privacy in the Digital Age: Perspectives on Analysis of Certain Central European Countries' Legislation and Practice*

András Zs. *Varga* – Lilla *Berkes* (eds.): *Common Values and Constitutional Identities—Can Separate Gears Be Synchronised?*

2024

Zoltán *Nagy* (ed.): *Economic Governance: The Impact of the European Union on the Regulation of Fiscal and Monetary Policy in Central European Countries*

Tímea *Barzó* (ed.): *Demographic Challenges in Central Europe: Legal and Family Policy Response*

János *Bóka* (ed.): *The Supranational Interpretation of the Rule of Law*

Contents

Notes on the Contributors

Editors and Authors

Katarzyna Zombory, PhD, is the director of research at the Central European Academy (CEA) in Budapest. In 2022, she led the establishment of the CEA as its acting director general. Prior to that, she worked at the Ferenc Mádl Institute of Comparative Law in Budapest. She graduated from the Maria Curie-Skłodowska University in Lublin, Poland, with a degree in law, and has also taken courses at the Centre Européen Universitaire de Nancy, The Hague Academy of International Law, the University of Leiden, and the Pázmány Péter Catholic University in Budapest. She holds a PhD in public international law, and her current research field focuses on international human rights law. She is a member of several scientific societies (including the International Law Association–Hungarian Branch, and the Central European Association of Comparative Law), and on the advisory and editorial boards of journals (*Central European Journal of Comparative Law* and *Law, Identity and Values*) and for book series (Legal Studies on Central Europe, Studies of the Central European Professors' Network). She is also the chairwoman of the Human Rights Center of the Central European Association for Comparative Law.

János Ede Szilágyi, PhD, Prof., has served as the director of strategy of the CEA since the year of its creation, playing a cardinal role in its establishment. He is also a professor at the Faculty of Law of the University of Miskolc. He studied law at the University of Miskolc, where he obtained his PhD and habilitation, and where he has worked since the beginning of his professional career. In addition, between 2019 and 2024, he was Director of the Ferenc Mádl Institute of Comparative Law, a public research institute based in Budapest. He is a founding professor of the Central European Professors' Network and the Central European Junior Programme, and co-founder of CEA Publishing. He is the head of the Central European Comparative Law PhD programme at the Doctoral School of the University of Miskolc. He is the editor-in-chief of several journals (*Journal of Agricultural and Environmental Law*, *Central European Journal of Comparative Law*, and *Law, Identity and Values*) as well as book series (Studies of the Central European Professors' Network, Legal Studies on Central Europe, and Legal Heritage). He is a member of the board of directors of the European Public Law Organization, the Hungarian deputy delegate of the Comité Européen de Droit Rural, and the president of the International Scientific Advisory Body of the Central European Association for Comparative Law.

Authors

Tamás Csiki Varga, PhD, is senior research fellow at the John Lukacs Institute for Strategy and Politics of Ludovika, University of Public Service (Budapest, Hungary). Previously, he was policy analyst at the Institute for Strategic and Defense Studies, a Hungarian Ministry of Defence thinktank, for 14 years. At both institutions, he has undertaken security and defence policy analysis. His research focuses on European security and defence, encompassing NATO (National Atlantic Treaty Organization) and the United States' grand strategy, the defence policy of individual European countries (e.g. Germany), Central European defence cooperation, as well as Hungarian security and defence policy. As an author or contributor to more than 200 publications, including nine books, and 22 book chapters in security and defence, his expertise is backed by an established network of scholars in the field. At the strategic level, he was a participant in formulating national security and defence strategies, as well as contributing to various strategic foresight analysis processes for Hungary and NATO. His research in 2024 explores European defence industrial cooperation, the security and defence policy implications of Hungary's European Union (EU) presidency, and the effects of Russia's aggression against Ukraine on the armed forces' modernisation programmes of Central European countries. His latest major upcoming publication is 'Hungary's defence policy in the 21st century' (Magyarország védelempolitikája a 21. században), co-authored by Péter Tálas, a monograph outlining the trends and strategic processes formulating Hungarian defence in national and allied (NATO, EU) frameworks.

Stjepan Groš, PhD, is an associate professor of computer science at the Faculty of Electrical Engineering and Computing, University of Zagreb. He received his PhD in computer science from the University of Zagreb. His main research and professional interests are offensive and defensive cybersecurity. He participated in the development of the Smart specialisation strategy 2016–2020, where he led the definition of specialisation for the Republic of Croatia in cybersecurity. He is a member of the management board of the Croatian defence industry competitiveness cluster and a chair of Cyber and Information Security sessions at the MIPRO conference. In 2018 and 2019, he was a member of a task force that organized national cyber security exercises under the auspicies of the Ministry of Defence of the Republic of Croatia for the top-level government officials. He regularly participates in roundtable discussions on various cybersecurity topics.

Lieutenant Colonel **Attila Horváth** is a researcher at the Space Law and Policy Research Institute of the Ludovika National University of Public Service and a co-author of the space law textbook published by the institute. He is a titular associate professor at the University of Debrecen, where the first space systems operators' course for the Hungarian Defence Forces was developed. He is also a member of the Hungarian Association of Military Sciences. His research areas include military

space operations, the use of high-altitude platform stations to support military operations, and the use of nanosatellites in military and national security operations. His current assignment is as branch head of the Satellite Operations Capabilities Branch, Capability Development Office, General Staff of the Hungarian Defence Forces.

Marko Jurić, PhD, graduated from the Faculty of Law at the University of Zagreb in 2007 and received his PhD from the same institution in 2013. Starting as an assistant in 2007, he served as a senior assistant from 2013 and an assistant professor from 2016 before being appointed in 2022 as an associate professor at the University of Zagreb's Department of Information Technology Law. He was also the vice-dean of the Faculty of Law from 2017 to 2021. He regularly advises international organisations and business entities on personal data protection, cybercrime, and cybersecurity laws.

Barbara Kaczmarczyk, PhD, Dr. hab., is a habilitated doctor of social sciences in the discipline of security science and a colonel in the Polish Army. She has served in her country's Border Guard (2002–2012) and Police (2012–2014). She specialises in crisis management systems, state border protection, security education, information management, civil-military cooperation, and information operations. She is the leader of many research projects in the field of security. She is the author of 120 scientific publications, including five scientific monographs, a scientific editor of several scientific monographs, and the author and co-author of several dozen scientific articles published in Poland and abroad.

Bálint Kovács is an assistant lecturer at the Faculty of Law and Political Science, University of Szeged, where he teaches international economic law, private international law, and the law of regional economic integration. He has also been teaching international economic law at the Sapientia Hungarian University of Transylvania since 2017. His PhD at the University of Debrecen focuses on small and medium-sized investors' access to investor–state dispute settlement. Since 2022, he has been a visiting lecturer at the University of Miskolc teaching international commercial arbitration. He is also a researcher at the Ference Mádl Institute of Comparative Law, where he has been conducting comparative legal research on private and international investment laws. His other fields of interest include economic security, defence industrial policy, and the human rights of national minorities.

Kaja Kowalczewska, PhD, is an assistant professor at the Academic Excellence Incubator, Centre for Digital Justice, at the Faculty of Law, Administration and Economics of the University of Wroclaw. She received her PhD in legal sciences with a specialisation in international law from the Faculty of Law and Administration at Jagiellonian University in Kraków (2019). She was a visiting researcher at the University of Melbourne (2017) and University of Cologne (2022). She is a member of the Commission for the Dissemination of International Humanitarian Law of the

Polish Red Cross. She was the author of the first Polish monograph dedicated to the use of artificial intelligence (AI) in armed conflicts. Her primary fields of interest are international humanitarian law, criminal law, and new technology.

Katarzyna Malinowska, PhD, Dr. hab., is an associate professor at Kozminski University and an expert in risk management and insurance, including space insurance. She is the author of several publications in the field, including the book *Space Insurance: International Legal Aspects* (Kluwer Law International, 2017). Her research focuses on risk prevention and management in the context of sustainable space operations. A frequent speaker at national and international conferences, she is also the director of the Centre for Space Studies at Kozminski University and head of the post-graduate programme Entrepreneurship in the Space Industry. She serves as an expert in the Polish Space Agency (POLSA) on space liability and insurance regulations and on the implementation of national space law. She is also a member of the Enterprise Risk Management Committee of the International Astronautical Federation, International Institute of Space Law, and European Centre for Space Economy and Commerce (ECSECO).

Krzysztof Masło, PhD, is an assistant professor at the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw. His research areas include international criminal law, the law of armed conflict, state jurisdiction, contractual law, and the EU area based on freedom, security, and justice. He is also a prosecutor specialising in economic crimes and international legal cooperation in criminal matters.

Jan Mazal, PhD, is an associate professor of military management and, since 2020, has been the chief of the Military Robotics Department at the University of Defence in Brno. He received his PhD in defense management in 2013. He is an author or co-author of over 80 scientific publications, robotic prototypes, and various professional software applications. He is the annual chairman or organizer of scientific conferences (MARS – Military Advanced Robotic Systems, MESAS – Modelling and Simulation for Autonomous Systems, I3M, etc.), Czech national representative in the NATO Science and Technology Organization – Applied Vehicles Technology Panel, Chairman of the Czech Ministry of Defence Council for AI and Robotics, and a member of several NATO working groups (MCDC-Multinational Capability Development Campaign, NATO Science and Technology Organization, Land Capability Group/Land Engagement/Team of Experts for Unmanned Ground Vehicles). His expertise includes military robotics, C4ISR systems, and modeling and simulation in the military domain.

Anna Molnár, PhD, Prof., is a professor at the University of Public Service (Budapest) and the head of the Department of International Security Studies. She is the head of the international security and defence studies bachelor's and master's

programmes. She was responsible for the international public management bachelor's programme and the international public service relations master's programme at the University of Public Service (2016–2021). She was the head of the programme for the MA in international studies at the University of Pannonia (Institute of Social Sciences and International Studies, Veszprém; 2010–2013). She received her PhD in international relations from the Corvinus University of Budapest (2003). Her research interests include the EU common foreign and security policy, common security and defence policy, and Italian history and politics. She became a visiting professor at the University of Rome (La Sapienza) in 2023. She has been actively participating in the European Security and Defence College since 2013.

Grzegorz Ocieczek, PhD, is an assistant professor at the Faculty of Law in the Department of Criminal Procedure at UKSW Cardinal Stefan Wyszynski University in Warsaw. He is a retired prosecutor of the National Prosecutor's Office, a colonel of Special Services, former Deputy Head of the Internal Security Agency, and the Central Anti-Corruption Bureau. He is a member of the Polish Platform for Internal Security, helping create advanced, integrated technological tools to support the activities of law enforcement agencies and the judiciary. He was a participant in the International Visitor Leadership programme organised by the United States Department of State in the field of combating crime and terrorism. He has published 30 articles on the topic of organised crime and crown witnesses.

Brigadier General **Andrzej Pawlikowski**, born 15 October 1969 in Zakopane, Poland, graduated from the Cracow University of Technology and the National Defence University of Warsaw/Rembertów. He has extensive experience in special units under Poland's Prime minister as well as minister of the interior and administration. He headed the Government Protection Bureau twice and played a key role in establishing the State Protection Service in 2018. He has held positions such as head of direct security for the minister of foreign Affairs, and chairman of the Organization for Security and Co-operation in Europe. He co-founded BINASE and became an advisor to the president of Poland in 2015. Currently, he is a professor and director of the Strategic Studies Institute at the War Studies University. He has also served as the vice president of the Polish American Alumni Association since June 2023.

Iztok Prezelj, PhD, Prof., is a professor and dean at the Faculty of Social Sciences, University of Ljubljana, Slovenia. As vice-dean for scientific research, he led the research process at the Institute of Social Sciences with 20 research centres from 2017 to 2021. From 2015 to 2017, he was also the chair of defence studies. He has published widely in the fields of threat and risk assessment, national and international security, crisis management, terrorism and counterterrorism, intelligence studies, and critical infrastructure. He has been a visiting researcher or lecturer at Princeton University (2017, 2018, 2019), Leiden University (2017), the University of Sarajevo (2012), the University of Vienna (2013, 2015), and the WEU Institute for Security

Studies in Paris (1997). He was an adjunct professor in the programme on terrorism and counterterrorism (PTSS) in 2014 at the George C. Marshall European Center for Security Studies in Garmisch, Germany. He is also president of the Euro-Atlantic Council of Slovenia.

Miha Šepec, PhD, is an associate professor and the head of the Institute for Criminal Law at the University of Maribor's Faculty of Law. He graduated in 2010 and earned his doctoral degree from the Faculty of Law, University of Maribor in 2015 on the topic of cybercrime. He is the sole editor of the *Commentary on the General Part of the Slovene Criminal Code* (2021) and the *Commentary of the Criminal Procedural Act* (2022). He has co-ordinated European Investigation Order: Legal Analysis and Practical Dilemmas of International Cooperation (EIO-LAPD), a project funded by the European Commission's Justice programme. He has published more than 200 articles on criminal law, procedural law, and cybercrime.

János Székely, PhD, has been a senior lecturer at the Sapientia Hungarian University of Transylvania's Department of Legal Science since 2017, and was a junior lecturer at the same institution from 2012. He earned his PhD in law from the University of Debrecen's Faculty of Law's Géza Marton School of Doctoral Studies in 2017. His research topics include the history of civil law and civil procedure, comparative civil and procedural law, current civil procedure and inheritance law, technological law, and the regulation of emerging and foundational technologies such as artificial intelligence, a topic on which he has organised several international scientific conferences. He is the author or co-author of three books each in Romanian and Hungarian, and numerous scientific articles and book chapters in Hungarian and English.

Colonel **Zvonko Trzun**, PhD, is the head of the Department of Polytechnics at the Dr. Franjo Tuđman University of Defence and Security in Zagreb, Croatia. Previously, he held several leading positions at the Croatian Military Academy, including vice-dean for science and development and head of the Department of Military Technology. His expertise covers multiple military subjects, such as ballistics, drones, modern weapons, and ammunition. In addition, Colonel Dr. Trzun actively participates in military study programmes across all branches: Land, Air Force, and Navy. Over the years, he has authored numerous studies on external ballistics, weapon usage, and the development of military technologies. His publications also address defense strategies against hybrid warfare and other military-related dangers.

Reviewers

Tomasz Długosz
Assistant Professor, Jagiellonian University, Poland

Jacek Dworzecki
Professor, Pomeranian University in Słupsk, General Tadeusz Kościuszko Military University of Land Forces, Poland

Karl-Heinz Gimmler
CEO, Gimmler law company and Gimmler Logistics Foundation; Lieutenant Colonel (Res), German Armed Forces, Germany

Norbert Grzesik
Professor, Military University of Technology, Poland

Attila Gulyás
Senior Researcher, National University of Public Service, Hungary

Miha Hafner
Assistant Professor, University of Ljubljana, Slovenia

Łukasz Kułaga
Professor, Cardinal Stefan Wyszynski University in Warsaw, Poland

Csongor István Nagy
Professor, University of Szeged, Hungary

Magdalena Pacholska
Postdoctoral Researcher, T.M.C. Asser Institute, The Netherlands

Grzegorz Pilarski
Professor, War Studies Academy in Warsaw, Poland

Małgorzata Polkowska
Professor, War Studies Academy in Warsaw, Poland

Zoltán Szenes
Professor, National University of Public Service, Hungary

Katarína Šmigová
Associate Professor, Dean of the Faculty of Law, Pan-European University, Slovakia

Csongor Balázs Veress
Assistant Professor, Károli Gáspár University of the Reformed Church in Hungary, Hungary

Emőd Veress
Professor, University of Miskolc, Hungary

Milan Vrdoljak
Professor, University of Zagreb, Croatia

Marin Vuković
Assistant Professor, University of Zagreb, Croatia

Marcin Wielec
Professor, Vice-Dean of the Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw, Poland

---

Technical Editor

Błażej Tazbir
PhD student, Deák Ferenc Doctoral School of Law, University of Miskolc; Intern, Central European Academy

'Si vis pacem, para bellum'

Developing the EU Legal Framework for the Defence Industry

Katarzyna Zombory and János Ede Szilágyi

In the wake of a changing global security environment and recent conflicts in Europe, it has become imperative to establish a comprehensive and ambitious strategy for developing defence capacities and defence industries within the European Union (EU) and its Member States. In the recent decades, global military powers have augmented their defence budgets at a much higher rate than Europe. For example, between 1999 and 2021, EU's combined defence spending increased by 19.7%, compared to 65.7%, 292% and 592% in the United States, Russia and China, respectively.[1] Faced with new security threats, EU Heads of State or Government reinforced their commitment to bolstering European defence capabilities.[2] This includes closer cooperation at the EU level and developing domestic defence capabilities. By increasing their military capacities and building a robust domestic defence industry, EU Member States can strengthen their overall level of security, resilience, and defence capabilities, aiming for greater self-sufficiency and independence from external security providers.

1 Data from the European Commission, citing the Stockholm International Peace Research Institute (SIPRI), see: European Commission, High Representative of the EU for Foreign Affairs and Security Policy, Joint Communication on the Defence Investment Gaps Analysis and Way Forward, 18 May 2022, JOIN (2022) 24, para. 2.

2 The EU Heads of State or Government during the meeting in Versailles in March 2022 committed to bolstering European defence capabilities by 1) increasing defence expenditures; 2) enhancing cooperation through joint projects; 3) addressing shortfalls and meeting capability objectives; 4) boosting innovation, including through civil/military synergies; and 5) strengthening and developing the EU defence industry, including SMEs, see: European Commission, High Representative of the EU for Foreign Affairs and Security Policy, Joint Communication on the Defence Investment Gaps Analysis and Way Forward, 18 May 2022, JOIN (2022) 24.

Katarzyna Zombory and János Ede Szilágyi (2024) 'Developing the EU Legal Framework for the Defence Industry'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 23–32. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_0

From the outset, the legal framework of European integration, which led to the creation of the EU, has been founded on pacifist premises, aiming to prevent future full-scale armed conflict through economic cooperation among *peace-loving states*.[3] Nevertheless, global security challenges in the second and third decades of the 21st century have intensified the need for a careful review of the *acquis unionaire* and its adaptation to new circumstances, so that the EU legal framework and its integration model can create conditions conducive to the development of European and national military industries. However, developing the arms industry raises several legal concerns across various areas of law. Some of these concerns will be explored in this book, focusing specifically on international and EU laws and, to a lesser extent, the domestic legal frameworks of Member States. The scope of legal analysis associated with defence industrial development and the strengthening of the EU's defence dimension extends beyond the legal framework of the Common Security and Defence Policy (CSDP). It involves the legal regime governing international trade and investment and includes legal regulations concerning a wide range of innovative military technologies.

This book has a two-fold objective. First, the authors aim to identify and explore applicable legal framework; second, they seek to identify the uncharted areas and legal challenges that need to be addressed to enable the development of the European defence industry. Several authors have attempted to suggest potential improvement directions for European and domestic lawmakers alike (*de lege ferenda* proposals). However, at the current stage of research, these proposals can only be considered as a springboard for further debate.

This book is a collaboration between scholars representing various areas of science, such as law, military, security studies and engineering. The editors operated under the assumption that the research topic requires an interdisciplinary approach. While drafting the research concept, the editors faced the challenge of harmonising various methodological approaches employed by scholars from diverse fields of science. They accomplished this task with varying results in different parts of the book, and it is left to the reader to evaluate the final outcome.

The book is divided into five parts, and its structure is as follows. Part I (*Policy and Technological Background*) provides insights into the following policy issues: the EU's common defence and security policy in light of national defence policies; challenges and perspectives for the development of the defence industry in EU and Member States; and challenges and breakthroughs in military innovation. Part II (*The CSDP and Law*) presents an overview of the legal environment surrounding the CSDP, while Part III (*Legal Aspects of Investment and Financing*) outlines the legal

3 The authors refer to the term used in the Preamble of the Charter of the United Nations, signed on 26 June 1945 in San Francisco. The EU has become a defence alliance, in addition to an organisation of economic and social integration with the adoption of the Lisbon Treaty, an expression of which was the inclusion of the mutual defence clause in the new Article 42, para. 7 of the Treaty on European Union.

framework governing defence industrial development, as well as investment and financing aspects. Part IV (*Fields of Innovations and their Legal Regimes*) offers a balanced overview of, on the one hand, the legal aspects associated with certain military innovation areas of crucial importance to the defence industry, and on the other hand, insights from their practical application. Part V (*Critical Infrastructure Protection*) addresses issues related to the protection of critical infrastructure in the EU.

In her contribution, *Anna Molnár*[4] discusses the institutional framework of the CSDP, one of the EU's youngest policy areas, considering the historical background of European integration in the fields of foreign, security, and defence policies. Molnár focuses on European strategic autonomy and European Defence Union, while exploring how this is reflected (or not) in the domestic defence policies of EU Member States.

Tamás Csiki Varga[5] presents the dynamics of the changing European security environment and threat perceptions, and provides an assessment of European military and defence industrial capabilities. Varga identifies capacity gaps and evaluates EU policy responses, including improved defence investments, to elucidate the demand–supply equation of the EU defence industry in 2024. He summarises his evaluation through an illustrative SWOT analysis of the EU's Defence Technological and Industrial Base (EDTIB).

Andrzej Pawlikowski[6] explores the evolving landscape of military technologies in EU Member States and compares these with recent military developments in the United States, China and Russia. Pawlikowski examines the potential implications of emerging military technologies for warfare, from the tactical intricacies of military operations to ethical considerations. He formulates recommendations for policymakers and defence experts in EU Member States to ensure that emerging military technologies contribute to global peace, stability and shared prosperity.

Krzysztof Masło[7] outlines the legal framework of the Common Foreign and Security Policy (CFSP), anchored in both primary and secondary EU law. Masło comprehensively examines EU competence in the field of CFSP, including civilian and military crisis management, CFSP's institutional structure, and decision-making processes. He addresses the issue of sovereignty of EU Member States within the CFSP context, and examines the legal foundations and historical background of the strategic partnership between the CFSP and the North Atlantic Treaty Organization.

Bálint Kovács[8] analyses EU laws relevant to improving common defence capabilities by encouraging industrial development. Kovács assesses their practical application and implementation by EU Member States and highlights the challenges

4 Molnár, 2024.
5 Csiki Varga, 2024.
6 Pawlikowski, 2024.
7 Masło, 2024.
8 Kovács, 2024.

facing the European Defence Equipment Market. He evaluates whether classic principles of competition and market logic are conducive to creating an improved EDTIB, a suitable defence industry, and a strong defence force in the EU.

Jan Mazal and *János Székely* focus on dual-use technologies on contemporary battlefields. Mazal[9] explores state-of-the-art dual-use innovations and addresses the complex relationship between cutting-edge military technologies and their dual-use potential. Driven by the assumption that future conflicts will increasingly become hybrid and integrated with the civilian domain, he explores the benefits and potential future trajectories of interconnected technological developments and their various (social, psychological, cultural, ethical, political, and environmental) implications for military and civilian domains alike. Székely[10] analyses major regulatory frameworks applicable to dual-use technologies, and selected emerging and disruptive technologies, primarily under the Wassenaar Arrangement, as well as export control regimes of the EU, United States and China. Székely explores the implications of regulations on dual-use technology transfer for international trade and business in the context of economic policy securitisation. He highlights the risks and challenging legislative gaps associated with dual-use governance in a field dominated by economic and military rivalry between global technological powers.

Iztok Prezelj and *Marko Jurić* focus on the use of Artificial Intelligence (AI) in contemporary military conflicts. Prezelj[11] demonstrates the broad spectrum of potential or actual use of AI by the armed forces and addresses related challenges and risks. He identifies the main geopolitical and strategic concerns surrounding the development and use of AI systems, particularly regarding implications for the balance of global power, and examines the approach of EU Member States to AI-enabled defence innovation. Jurić[12] analyses whether the existing EU legal framework covers the use of AI in military and defence sectors. He discusses general legal regulations on AI, with a closer analysis of the EU Artificial Intelligence Act, and examines the case law of the Court of Justice of the European Union (CJEU) to unveil its position on the applicability of EU law in the military context. He also explores the impact of EU data protection rules, primarily the General Data Protection Regulation (GDPR), on the use of data in AI activities within military and defence contexts, and identifies the challenges in the development and use of AI within the existing legal environment.

Attila Horváth and *Katarzyna Malinowska* examine the evolving landscape of military activities in outer space and the practical legal implications of rapid technological advancements in this area. Horváth[13] demonstrates that advances in technology and operations have outpaced the legal regime, endangering the peaceful and

9 Mazal, 2024.
10 Székely, 2024.
11 Prezelj, 2024.
12 Jurić, 2024.
13 Horváth, 2024.

sustainable long-term use of outer space. He raises several legal and sustainability concerns, connected but not limited to the delimitation of airspace and outer space, operations in the border region, sovereignty, and zoning of outer space related to spacecraft, as well as the operations of active spacecraft, the removal of inactive spacecraft and space debris. Malinowska[14] outlines the legal framework governing the military and defence use of outer space at international and national levels and explores the possible application of space law principles. She addresses the idealised vision of outer space as the common heritage of mankind for peaceful purposes in the wake of militarisation and weaponisation of space, as well as such critical issues as close-proximity operations, cyberattacks on space infrastructure, and anti-satellite weapons (ASAT) tests.

Zvonko Trzun and *Kaja Kowalczewska* address different aspects of the military's use of unmanned warfare. Trzun[15] provides an overview of the development and current capabilities of unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs) while elucidating the technical limitations and risks associated with their deployment, particularly in terms of reliability, targeting process, and excessive lethality. He highlights the lessons drawn from the 2022 Russo-Ukrainian War, and explores current trends in Europe for the acquisition of drones and robots. Kowalczewska[16] outlines the relevant legal regime and addresses the legal complexities surrounding the use of unmanned platforms under the UN Charter, the law of armed conflicts, international human rights, and international criminal laws. She particularly focuses on the legal review of weapons before deployment, the use of unmanned platforms beyond the theatre of active armed conflict, and contentious combat methods such as targeted killings and signature strikes.

Barbara Kaczmarczyk and *Miha Šepec* explore various aspects of cyberwarfare, indicating the pressing need for EU cooperation in cybersecurity. Kaczmarczyk[17] demonstrates the evolution of cyber threats, illustrating them with several case studies, such as the 2007 cyber-attack in Estonia and the 2010 Stuxnet attack. She examines the causes and effects of cyber-attacks, and presents their implications for national security, demonstrating how cyberspace has become a genuine battlefield. Meanwhile, Šepec[18] analyses international and EU legal frameworks relevant to cyberwarfare attacks and procedural measures of cooperation in criminal matters for the purpose of prosecuting cybercrimes. He assesses whether there is a need to amend existing EU legislation or adopt new EU instruments at the criminal material level to cyberwarfare.

Stjepan Groš and *Katarzyna Zombory* address hybrid threats and warfare and their inherent element: information warfare. Groš[19] explores the anatomy of infor-

14 Malinowska, 2024.
15 Trzun, 2024.
16 Kowalczewska, 2024.
17 Kaczmarczyk, 2024.
18 Šepec, 2024.
19 Groš, 2024.

mation operations and presents the tactics and techniques used by hybrid adversaries in military domains and information spaces. His analysis assumes that countering disinformation requires deep insight into the characteristics and dynamics of information operations; therefore, he also attempts to define parameters to identify different types of threat sources and threat actors. Zombory[20] performs a legal analysis of hybrid threats and warfare under international law and questions whether the use of hybrid hostilities is tantamount to the use of force and whether it triggers legal consequences related to the existence of armed conflict. She aims to establish the scope of lawful countermeasures available to affected states and outlines the EU policy and legal framework relevant to countering hybrid threats.

Grzegorz Ocieczek[21] addresses the issue of critical infrastructure protection and demonstrates that it requires an interdisciplinary approach, combining perspectives from various disciplines, such as law, security studies, and social and public policy. He explores the concept of critical infrastructure and outlines the relevant international and EU legal frameworks, underpinned by the assumption that the protection of critical infrastructure is closely linked to public safety and counterterrorism.

The findings suggest that introducing a coherent, common legal framework conducive to the development of the EU defence industry may be challenging for several reasons. Years of underspending on defence have resulting in an accumulation of shortfalls in collective military inventories, reducing the industrial production capacity of EU Member States.[22] The varying economic interests and differing defence priorities of Member States do not create a favourable environment for adopting a common legal framework for military industrial development. This is especially true given the complexities in determining the nature and scope of the EU's competences in the areas of CFSP and CSDP, where the dynamics of European integration are shaped by the duality of intergovernmentalism and supranationalism.[23]

Regarding the research and development of new military technologies, it has been demonstrated that, technological innovations often outpace legal regulations.[24] Divergent state approaches and distinct combat strategies have resulted in a lack of unified, binding positions on the acquisition or development of certain military technologies, such as unmanned warfare, which hampers legislative processes within the EU.[25] Significant challenges in the development and use of new technologies in the military domain may arise from existing EU regulations, as in the case of AI and the EU legal regime governing the use of personal data. Current EU rules on data processing also apply to the military sector, and can seriously affect the ability of national military forces to process certain types of data.[26] Any proposed regulatory

20 Zombory, 2024.
21 Ocieczek, 2024.
22 Csiki Varga, 2024; Balint Kovács, 2024.
23 Masło, 2024; Molnár, 2024.
24 See eg. Jurić, 2024; Székely, 2024; Malinowska, 2024; Kowalczewska, 2024.
25 Kowalczewska, 2024.
26 Jurić, 2024.

framework should be integrated into existing legal regimes.[27] While creating a legal regime governing military innovations, especially dual-use technologies, legislators must balance overly permissive and restrictive norms, even if this is likely to impact economic securitisation.[28] It is crucial to consider that new military technologies may raise not only legal but also serious ethical concerns; therefore, it is suggested that legal governance should be complemented by voluntary compliance and ethical standards.[29]

This research was conducted within the framework of the Central European Professors' Network of the Central European Academy in connection with the Hungarian EU Presidency in 2024. The participants hope that their scientific contribution will draw attention to the significance of the topic and the timeliness of the action.

27 Prezelj, 2024.
28 Székely, 2024.
29 See e.g. Mazal, 2024; Prezelj, 2024; Trzun, 2024.

References

Csiki Varga, T. (2024) 'Reinforcing European Defence Industry for Times of Great Power Conflicts' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 73–108; https://doi.org/10.54237/profnet.2024.zkjeszcodef_2.

Groš, S. (2024) 'Information Warfare Tactics and Techniques' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 701–754; https://doi.org/10.54237/profnet.2024.zkjeszcodef_16.

Horváth, A. (2024) 'Challenges of Practical Space Operations Under the Outer Space Treaty: Operations in a Legal Regime of a Different Era' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 437–478; https://doi.org/10.54237/profnet.2024.zkjeszcodef_10.

Jurić, M. (2024) 'Legal Aspects of Military and Defence Applications of Artificial Intelligence Within the European Union' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 395–436; https://doi.org/10.54237/profnet.2024.zkjeszcodef_9.

Kaczmarczyk, B. (2024) 'Cyberattacks/Incidents and Responding to Them' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 619–662; https://doi.org/10.54237/profnet.2024.zkjeszcodef_14.

Kovács, B. (2024) 'Legal Aspects of Defence Procurement in the European Union: Funding Incentives and Regulatory Shields' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 215–258; https://doi.org/10.54237/profnet.2024.zkjeszcodef_5.

Kowalczewska, K. (2024) 'Legal Aspects of Unmanned Warfare and Military Drone Operations' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 581–618; https://doi.org/10.54237/profnet.2024.zkjeszcodef_13.

Malinowska, K. (2024) 'Legal Aspects of Military and Defence Use of Outer Space' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 479–526; https://doi.org/10.54237/profnet.2024.zkjeszcodef_11.

Masło, K. (2024) 'Common Security and Defence Policy: A Legal Framework for Developing the European Defence Industry' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 161–214; https://doi.org/10.54237/profnet.2024.zkjeszcodef_4.

Mazal, J. (2024) 'The Dual Use of Civilian and Military Technologies in the Battlefield of the Future' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 259–308; https://doi.org/10.54237/profnet.2024.zkjeszcodef_6.

Molnár, A. (2024) 'The EU's Common Security and Defence Policy in the Context of European Strategic Autonomy' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 35–72; https://doi.org/10.54237/profnet.2024.zkjeszcodef_1.

Ocieczek, G. (2024) 'Selected Legal Aspects of National Security and Critical Infrastructure Protection in the European Union with Particular Reference to the Polish National Legislation' in the Legal System of the European Union' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 803–840; https://doi.org/10.54237/profnet.2024.zkjeszcodef_18.

Pawlikowski, A. (2024) 'Emerging and Innovative Military Technologies in the EU Member States: Background and Issues' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 109–160; https://doi.org/10.54237/profnet.2024.zkjeszcodef_3.

Prezelj, I. (2024) 'The Use of Artificial Intelligence-Enabled Systems by Modern Armed Forces and Some Related Concerns' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 357–394; https://doi.org/10.54237/profnet.2024.zkjeszcodef_8.

Šepec, M. (2024) 'Legal Aspects of Cyberwarfare and Cyberwarfare Crimes: Criminal Law Analysis and Dilemmas' in the Legal System of the European Union' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 663–700; https://doi.org/10.54237/profnet.2024.zkjeszcodef_15.

Székely, J. (2024) 'Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 309–356; https://doi.org/10.54237/profnet.2024.zkjeszcodef_7.

Trzun, Z. (2024) 'Robots and Drones on Battlefields: New Capabilities and Emerging Challenges' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 527–580; https://doi.org/10.54237/profnet.2024.zkjeszcodef_12.

Zombory, K. (2024) 'Legal Aspects of Hybrid Threats and Warfare' in Zombory, K., Szilágyi, J.E. (eds.) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*. Miskolc-Budapest: Central European Academic Publishing, pp. 755–802; https://doi.org/10.54237/profnet.2024.zkjeszcodef_17.

Part I

POLICY AND TECHNOLOGICAL BACKGROUND

Chapter 1

The EU's Common Security and Defence Policy in the Context of European Strategic Autonomy

Anna Molnár

Abstract

In the wake of a worsening global security environment, the concepts of European strategic autonomy, open strategic autonomy, strategic sovereignty or the European Defence Union are becoming increasingly relevant. In addition to economic power, there has been a growing demand in recent years for the European Union (EU) to become a military power, thereby enhancing its ability to act autonomously. It is important to emphasise that these concepts cover not only the defence sector but also the fields of economy, digitalisation, and technological innovation.

In this chapter, I will first briefly introduce the historical background of the Common Security and Defence Policy (CSDP). I will then provide an overview of its theoretical background by examining the concept of the European Defence Union. Following this, I will elucidate the current state of new initiatives related to European defence in connection with the accelerated integration process. Finally, I will map national defence policies regarding European strategic autonomy. As the concept of the European Defence Union has been promoted primarily by EU institutions and finds no mention in Member States' strategic documents, the aim of the last subchapter is to analyse Member States' perceptions regarding the concept of European strategic autonomy (EU-SA). This part of the research is based on secondary literature and an analysis of the latest national security strategic documents, particularly those of Member States.

Anna Molnár (2024) 'The EU's Common Security and Defence Policy in the Context of European Strategic Autonomy'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 35–72. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_1

Member States have expressed diverse opinions regarding EU-SA, which was originally associated with security and defence policies. Today, it has an extended meaning that includes economic, technological and energy policies. The National Security Strategy (NSS) of one group of Member States (such as France or Italy) has prioritised EU-SA, while another group (such as the Netherlands) has developed the concept of open strategic autonomy (OSA), and the documents of a third group (such as the V4 countries) neither mention EU-SA nor OSA. The last group of Member States represents a more transatlanticist view of security and defence.

Keywords: European strategic autonomy, European Defence Union, defence initiatives, security, power

1. Introduction

The Hungarian presidency of the Council of the European Union and the 25th anniversary of the European Union's (EU) Common Security and Defence Policy (CSDP) in 2024 provide an opportunity to review the development of this special policy area within the EU. Over the last few decades, not only the institutional system, decision-making processes, and crisis management structures of the CSDP, but also the concepts of the European Defence (and Security) Union and European strategic autonomy (EU-SA) have repeatedly emerged. The unprovoked Russian invasion of Ukraine has accelerated this process, enhancing the defence characteristics of the EU and strengthening transatlantic relations.

Considering the deteriorating global security environment, the concepts of EU-SA, open strategic autonomy, strategic sovereignty, or the European Defence Union (EDU) have become more relevant than ever. Furthermore, in addition to the EU's economic power, there has been growing demand for the EU to become a military power, enabling it to act autonomously. It is important to emphasise that this concept covers not only the defence sector, but also the fields of economy, digitalisation and technological innovation.

First, I will briefly introduce the historical background of the Common Security and Defence Policy (CSDP); second, I will provide an overview of its theoretical background. I will discuss the following theories and concepts: differentiated integration, intergovernmentalism versus supranationalism, the power perception of the EU from normative to smart power, strategic autonomy, and European sovereignty. The theoretical section examines the concept of the EDU. Third, I will introduce the current state of new initiatives related to European defence in connection with the accelerated integration process. Finally, I will map national defence policies surrounding EU-SA. As the concept of EDU has primarily been promoted by EU institutions and is not mentioned in Member States' strategic documents, the aim of the last subchapter

is to analyse Member States' views on the EU-SA concept. This part of the research is based on secondary literature and an analysis of the latest national security strategic documents, particularly those of Member States.

2. Historical background

European integration has always been considered a security or peace project. On the one hand, following the devastating experience of the two World Wars, it was intended to prevent another war between Western European States; on the other, it was clearly developed in the shadow of the Soviet military threat. During the 1950s, especially after the failure of the Pleven Plan for the creation of the European Defence Community (EDC) in 1954, traditional areas of diplomacy, security and defence were not initially included in the treaties establishing the European Coal and Steel Community (1951) or the European Economic Community (1957). These areas remained entirely within the competence of Member States. The integration process essentially began in the economic field with the Treaties of Rome (1957). Despite this, various external relations instruments, such as enlargement policy, trade policy, development or humanitarian aid, and crisis response coordination, have steadily evolved since the creation of European Communities.

The EU was created by the Maastricht Treaty in 1992, establishing its three pillars: European Communities, Common Foreign and Security Policy (CFSP) and cooperation in the fields of Justice and Home Affairs. The first pillar is based on community decision-making, while the second and third concern intergovernmental decision-making. In 1997, the Treaty of Amsterdam introduced the position of High Representative for the CFSP, who was also the Secretary-General of the Council (SG/HR) of the EU, to strengthen the effectiveness of CFSP and to form a unanimous opinion in international relations. The EU's first High Representative for the CFSP was former North Atlantic Treaty Organization (NATO) Secretary-General and former Spanish Foreign Minister Javier Solana, serving between 1999 and 2009. The Treaty of Amsterdam also established the concept of constructive abstention in CFSP. This flexible instrument allows the EU to proceed with a decision even when a Member of State abstains.

2.1. Crisis management structures

In parallel with the development of the Common Security and Defence Policy (CSDP), the issue of security and defence gradually became a part of the integration process. Following intense discussions surrounding European defence, the debate regarding the future role of Western European Union (WEU) commenced. The Yugoslav wars in the 1990s highlighted the fact that, practically, the EU did not have

the right tools for crisis management outside its borders. The devastation following these wars prompted European leaders to initiate the integration of European defence, breaking the taboo on closer defence cooperation that developed after the failure of the EDC in 1954.[1] The Yugoslav wars became the driving force for deeper cooperation. A milestone in this process was the Saint-Malo Declaration by France and the United Kingdom in 1998, which emphasised that the EU must have the capacity for autonomous action.[2] In 1999, the European Council began discussions on the creation of a European Security and Defence Policy (ESDP).

The integration of the WEU into the EU led to the establishment of the European Security and Defence Policy (ESDP). In the early 2000s, with the Treaty of Nice, the establishment and institutionalisation of the ESDP began. Within the decision-making structure of the Council of the EU, military and civilian crisis management decision-making bodies were established: the Political and Security Committee (PSC), European Union Military Committee (EUMC), Civilian Crisis Management Committee, European Union Military Staff, and Political Military Group (PMG). The CSDP is the latest policy area of the EU. In 2003, the EU launched its first CSDP mission and operations, and the first European security strategy was adopted the same year. The creation of ESDP in the early 2000s led to the development of the EU Battlegroup (EUBG). The origin of the EUBG concept can be traced back to several bilateral summits and declarations (Franco–German, Franco–British, UK–Italy) but especially to a Franco–British proposal inspired by the successful implementation of the first autonomous EU crisis management operation, the Artemis military operation in the Democratic Republic of the Congo[3]. On 17 May 2004, the Council of the European Union adopted the "Headline Goal 2010", which was endorsed by the European Council in June 2004. This document set a target for establishing EUBGs and achieving full operational capabilities by 2007.[4] The final Battlegroup concept was completed in 2006. The EUBG is a multinational integrated force of at least 1,500 personnel, deployable within 10 days and up to 6,000 km for a minimum of 30 and a maximum of 120 days. In 2004, Member States offered to establish a total of 13 EUBGs. Within the framework of the Lisbon Treaty, EUBGs can be used for conflict prevention, initial stabilisation, humanitarian intervention and rescue operations, crisis management, and peacekeeping tasks. It is worth mentioning that, for financial and political reasons, the EUBGs have never been used for CSDP operations.

2.2. Capability development

However, from its early phase, the CSDP included not only crisis management but also capability development processes. Originally, the rules related to the internal

1 de Vasconcelos, 2009, pp. 15–26.
2 *Saint-Malo declaration*, 1998.
3 Missiroli, 2003, pp. 36–39.
4 Consilium, 2004.

market did not extend to the defence industry; thus, it remained fragmented, and the gradual integration of this economic field became necessary to create an open market and a competitive and effective defence industry. The first step was taken in 2003 when the European Commission initiated the gradual creation of a "European Defence Equipment Market" as an objective by establishing a more open market among Member States, which was of strategic importance for the reinforcement of the European defence technological and industrial base.[5] The most important result of the institutionalisation of this area at the European level was the establishment of the European Defence Agency (EDA) in 2004. From the beginning, EDA played a decisive role in the development of Member States' defence capabilities and the creation of a competitive market for European defence equipment.[6] In 2007, the EDA issued its strategy for the European Defence Technological and Industrial Base (EDTIB). The objective of the strategy adopted by Member States was the gradual integration of national-level capability development and the defence market to improve supply security, thus creating capability improvement at the European-level to reduce fragmentation. The creation of a better-coordinated, more competitive defence market with less duplication was among the goals to better serve European defence policy.[7] However, during the first two decades of this century, EU Member States fulfilled these strategic objectives only to a limited extent. According to Schnitzl,[8] although in recent decades, EU Member States decided on a number of regulations inciting cooperation, for instance, defence procurement (European Parliament 2009/81) and guidelines for transfers inside the EU (European Parliament 2009/43), the level of cooperation did not help achieve the planned goals.

2.3. The Lisbon Treaty

The Lisbon Treaty (2007) can be considered a significant milestone in the development of CFSP and CSDP. It abolished the pillar structure of the EU, while providing the EU legal personality, so that it could conclude its international treaties. Following the Lisbon Treaty, the competence of EU and its Member States were clearly separated. One of the most significant features of the Lisbon Treaty was that it promoted a more transparent separation of competences between different levels of governance in the field of external policies. By abolishing the pillar system, the CFSP was no longer clearly separable from other external actions, yet it remained a special policy, which was an exception to all the general rules of functioning of the EU, according to the Treaty on the European Union (TEU) (Title V, Articles 21–46 TEU)[9].

5 Commission of the European Communities, 2004.
6 Council of the European Union, 2004.
7 European Parliament, Directorate-General for External Policies, 2013.
8 Schnitzl, 2023, p. 8.
9 *Treaty on the European Union*, Title V, Articles 21–46.

With the new Treaty, a closer link was established between EU's external policy areas. The changes to EU's institutional setup and decision-making processes brought greater coherence between the common commercial policy, development and cooperation policy and CFSP (and as an integrated part of it, the CSDP). At the institutional level, closer cooperation and coherence were guaranteed by the new post of High Representative for Foreign Affairs and Security Policy (also Vice President of the European Commission, HR/VP) and the establishment of the European External Action Service (EEAS). Not only was this policy area renamed from ESDP to CSDP, the Lisbon Treaty also introduced several significant provisions regarding CSDP (e.g. Article 42(7) on mutual assistance and Articles 42(6) and 46 on permanent structured cooperation (PESCO)).[10]

3. Theoretical background

The role of the EU as an international actor is determined by the fact that, according to the Treaties, intergovernmental cooperation remains the dominant form of decision-making in the fields of CFSP and CSDP. The dynamics of the European integration process have been defined by the duality between intergovernmentalism and supranationalism. Although in some areas of external action, for example, in the case of common trade policy, the EU decision-making processes are based on the community (or union) method; this is not applied to CFSP and CSDP, which continue to be ruled by unanimity (intergovernmentalism) as very sensitive policy areas for Member States. The contradiction in this duality promoted the development of the EU as a new hybrid political organisation characterised by a supranational entity. The Lisbon Treaty reinforced the hybrid political character of the EU through the creation of EEAS and the new position of High Representative of the Union for Foreign Affairs and Security Policy. Although CFSP and CSDP are among the least integrated policy areas of the EU, the Commission's role has started to grow steadily in recent years. Despite growing support for a more credible European defence, the period before the Global Strategy (2016) saw deeper cooperation mainly restrained amid concerns related to sovereignty and lack of trust among partners within the EU.[11]

One of the most important innovations of the Lisbon Treaty was the extension of differentiated integration to the field of CSDP. The Treaty created PESCO as a new, flexible instrument for enhanced cooperation with the aim of promoting interoperability, reducing capability shortfalls, and strengthening cooperation in the field of capability development. According to Article 42 (6) TEU, Member States with

10 Molnár and Csiki Varga, 2023.
11 Cîrlig, 2015, p. 5; Molnár, 2022; Molnár, 2023.

enhanced military capabilities that meet higher standards may establish PESCO. This type of partnership offers the possibility of enhanced cooperation and various forms of differentiated integration within the EU. Differentiation is a flexible solution that allows a certain number of Member States to proceed with deeper integration into a specific policy area, bridging the gap between the diverse political opinions of Member States.[12] The field of defence has always been characterised by the diverse political opinions of Member States. The creation and launch of CSDP missions and operations and the *à la carte* approach in taking part in the capability development projects of the European Defence Agency have been determined by differentiation; thus, it has been considered a pragmatic solution, enabling the EU to move ahead in the field of defence.[13]

The EU has been labelled a *sui generis* international organisation or a supranational form of integration.[14] According to this definition, the EU is a unique political entity that is different from any other international organisation, comprising sovereign states that share part of their sovereignty.[15] The EU is not a great power in the classical sense as it was created in opposition to the ideas of great powers. It has been described as a "civilian"[16] or a "soft" power.[17] Up until the launch of ESDP, in the early 2000s, the EU could not be conceptualised as a hard or military power. Manners describes it as "normative" power, which promoted the diffusion of the EU's norms in international relations.[18] Over the last few decades, it has been conceptualised as an ethical[19] or liberal power[20] in international affairs. With the introduction of ESDP/CSDP, the EU has been labelled as a smart power, which can combine "soft" and limited "hard" power tools.[21] However, the hybrid power of this foreign policy actor nevertheless provokes disputes.[22] In many cases, concepts related to the EU cannot be clearly isolated, but are often overlapping.

Following the launch of ESDP at the beginning of the new millennium, and especially after the entry into force of the Lisbon Treaty (2009), the perception of the EU has changed significantly. According to Smith (2005), civilian power is 'non-military, and includes economic, diplomatic and cultural policy instruments'. Therefore, she also claimed that the EU was no longer a civilian power, but 'somewhere along a spectrum between the two ideal-types of civilian and military power'.[23] In 2010,

12 European Parliament, 2018.
13 Törő, 2014, p. 66; De Neve, 2007; Von Ondarza, 2013; Howorth, 2019; Grevi et al., 2020; Blockmans, 2017.
14 Phelan, 2012.
15 Wallace, 1999; Brack et al., 2019; Bifulco and Nato, 2020; Phelan, 2012.
16 Duchêne, 1973, p. 19; Duchêne, 1972; Stavridis, 2001.
17 Hill, 1990.
18 Manners, 2002; Manners, 2006.
19 Aggestam, 2008.
20 Wagner, 2017.
21 Cross, 2011; Nye, 2023.
22 Tocci, 2008; Phelan, 2012; Moravcsik, 2010.
23 Smith, 2005, p. 17.

Moravcsik claimed that the EU has become a superpower, which is 'able to exert global influence across the full spectrum of power, from "hard" to "soft".' He claimed that Europe is the only region in addition to the United States that projects intercontinental military power and possesses a range of effective civilian instruments for power projection.[24] In 2016, Federica Mogherini, High Representative for Foreign Affairs and Security Policy, also characterised the EU as a superpower, which emerged as a global player relying on its economic power.[25]

Over the last few decades, the security environment and international systems have worsened significantly. Power competition has become a norm in international politics. After Russia's invasion of Ukraine, hybrid and traditional war returned to Europe. It is no coincidence that the EU had to adapt to major changes in international relations. The Global Strategy for Foreign and Security Policy (Global Strategy or GS), adopted in 2016, is the first tangible sign of this adaptation, referring to the EU's civilian or soft-power character, while also underlining that this soft power is no longer enough (European External Action Service 2016b, 44). GS represented a pragmatic approach, focusing on the state and societal resilience of the neighbourhood, and introduced the concept of "principled pragmatism" and the need for strategic autonomy. It uses the concept of strategic autonomy in connection with security and defence.[26] Although the 2016 Council Conclusions have already provided definitional guidelines, an official definition of the concept of strategic autonomy has yet to be developed at the EU level. This concept can be summarised as enabling the EU to ensure its own security and act autonomously on land, in the air, at sea, in space and cyberspace. In addition, the EU must be capable of projecting power, responding to external crises, and making independent decisions in the field of defence policy.[27] Member States have different interests and positions regarding these concepts.[28]

French President Emmanuel Macron introduced the concept of European sovereignty in September 2017. Instead of "strategic autonomy", Macron used the terms autonomous operating capability and European sovereignty in a general sense in the field of defence. According to his views, there are six key elements of European sovereignty: 1) security and defence, 2) control of borders, 3) partnership with Africa, 4) ecological transition, 5) digital technology and 6) industrial and monetary economic power.[29]

The 2018 State of the Union address by Jean-Claude Juncker, then president of the European Commission, attributed European sovereignty to the geopolitical situation. Juncker stated that it was time for Europe to seize the opportunity and play the role of a Union, in shaping global affairs as a more sovereign actor in

24 Moravcsik, 2010, p. 91.
25 European External Action Service, 2016a.
26 European Parliament, 2022, p. 2.
27 Biscop, 2017; Biscop, 2018; Varga, 2017; de Sutter, 2020, p. 14; Jones, 2020; Fiott, 2018.
28 Weitershausen et al., 2020; Grüll and Lawton, 2020; Recchia, 2020; Silva and Zachary, 2020; Molnár, 2022; Molnár, 2023.
29 Macron, 2017; European Parliament, 2022.

international relations. According to him, European sovereignty is derived from Member States' national sovereignty, and does not replace it. Shared sovereignty strengthens this relationship. He also emphasised that this process does not mean the militarisation of EU; it means becoming more autonomous and living up to the EU's global responsibilities.[30]

In 2019, the new President of the European Commission, Ursula von der Leyen proposed to lead a "geopolitical Commission" and Josep Borrell, the High Representative of the Union (HR/VP), indicated that the EU needed to 'learn the language of power'. Although the historical connotations of geopolitics are controversial, the new Commission embraces this concept.[31]

In 2022, the Strategic Compass adopted by the Council highlighted the need for creating strategic autonomy and technological sovereignty.[32]

4. The concept of European Defence Union

Analogous to the development of crisis management structures and the debate on EU's relations with NATO, the concept of a EDU and strategic autonomy has repeatedly emerged. In the last decade, various EU institutions and Member States have supported the acceleration of European security and defence cooperation. This cooperation was also strengthened by the fact that 23 EU Member States are also NATO members.

This accelerated process is driven by both external and internal factors. First, the events of the Arab Spring; second, Russia's invasion of Ukraine; third, mass migration and refugee crisis triggered by turmoil and armed conflicts in the EU's southern neighbourhood; and fourth, the growing hybrid threats. The worsening relationship between the EU and the United States during Donald Trump's presidency can also be considered an accelerating factor. The Brexit referendum is another essential reason for this process. Finally, the changing and deteriorating global security environment, which has led to new power competition in the arms race, cannot be overlooked.

The concept of EDU can be traced back to the European Convention on the Future of Europe in 2002, which prepared draft treaty establishing a Constitution for Europe (Constitutional Treaty). During a debate on the Constitutional Treaty, France and Germany proposed the creation of a European Security and Defence Union (ESDU). Although Belgium and Luxembourg supported this idea, more Atlanticist

30 Juncker, 2018.
31 Fiott, 2020, p. 1; Molnár, 2022; Molnár, 2023.
32 Council of the European Union, 2022.

EU Member States rejected it.[33] Therefore, the draft treaty establishing a Constitution for Europe did not mention the ESDU.[34] Following the failure of the Constitutional Treaty, the Lisbon Treaty was much less ambitious but introduced significant changes regarding CSDP.

In December 2013, the European Council held its first thematic meeting dedicated to defence, identifying priority actions for stronger cooperation.[35] In the coming years, the idea related to European defence that attracted immense public attention and debate was Juncker's announcement in March 2015 regarding the need for a common European army to face external threats.[36] The 2015 terrorist attacks in Paris also served as a stimulus for further support, as France pushed for activating the EU Treaty's mutual assistance/defence clause.[37]

The Global Strategy for the EU's Foreign Affairs and Security Policy (GS), adopted in June 2016, a few days after the British referendum, expressed the goal of strategic autonomy and strengthening the EU as a security community.[38] After years of immobility in the field of defence integration, the implementation of the GS commenced (e.g. the European Defence Action Plan (EDAP), NATO–EU cooperation, and the European Defence Fund (EDF)). These steps were further supported not only by the main EU institutions,[39] but also Member States.[40]

In 2017, the European Commission published the 'Reflection Paper on the Future of European Defence', highlighting that 'the foundations of the ESDU are gradually being built', and that it 'should encourage a stronger alignment of strategic cultures', as well as a common understanding of threats and appropriate responses. It will require 'joint decision-making and action, as well as greater financial solidarity at the European level'.[41] In September 2017, Juncker, in his annual State of the Union address, expressed that by 2025, the EU should become a full-fledged EDU.[42] Although the definition of ESDU or EDU remains unclear, the gradual realisation of deeper European defence cooperation began after the adoption of GS.

33 Nováky, 2017; Consilium, 2003.
34 *Treaty establishing a Constitution for Europe*, 2004.
35 Consilium, 2013.
36 *EU-Kommissionspräsident Juncker für europäische Armee*, 2015; *NATO is not enough, EU needs an army*, 2016; European Parliament, 2015, p. 5; European Commission, 2019.
37 European Parliament, 2016a; Molnár, 2018; Molnár, 2022.
38 European External Action Service, 2016b.
39 Juncker, 2016; European Parliament, 2016b.
40 Ischinger, 2013; *Im Wortlaut, Pressekonferenz von Bundeskanzlerin Angela Merkel und Präsident Emmanuel Macron beim 19. Deutsch-Französischen Ministerrat* [Text of the press conference by Federal Chancellor Angela Merkel and President Emmanuel Macron at the 19th Franco-German Council of Ministers], 2017; Renzi, 2018; Partito Democratico, 2018; Grevi, 2016.
41 European Commission, 2017, p. 11.
42 Juncker, 2017.

Member States' governments and institutions elaborated on the first threat analysis in 2020, which led to the adoption of the Strategic Compass in 2022.[43] In February 2021, the President of the European Commission, at the video conference of the European Council, emphasised the need to create an EDU on building blocks such as PESCO, financially supported by EDF.[44] In 2021, the State of the Union address referred to the need for EDU, stating that, although the EU has started to develop a European defence ecosystem, there is nevertheless room to proceed.[45]

In March 2022, the Council of the EU adopted the Strategic Compass, a new strategic document. Germany and France played key roles in initiating and finalising it. Therefore, it is no coincidence that the process started in 2020 under the German Presidency of the Council of the EU and concluded in 2022 under French Presidency. The Strategic Compass, which focuses on the main issues of European defence incorporating reflections on the Russian invasion of Ukraine, covers four "baskets": crisis management, partnership, resilience and capability development. Based on a common threat assessment, the document sets out objectives for the EU and its Member States for the next 5–10 years. The Strategic Compass provides strategic guidance in the four areas based on an analysis of a common European understanding of threats and challenges. In light of the Russian invasion of Ukraine, during the informal meeting of the European Council on 10–11 March in Versailles, EU heads of state and the government adopted the Versailles Declaration, an outcome of which concerns the strengthening of European defence capabilities and the defence industry.[46]

Member States are facing increasingly complex security threats, and the level of the EU's "security and defence ambition" is increasing. Despite not being a genuine European military White Paper, the Strategic Compass was the first document designed to provide clarity, guidance, and incentives for the completion of a truly common security and defence policy (EDU). EU institutions and High Representative play key roles in the process driven by Member States.

In 2023, the State of the Union Address noted that the EU has launched efforts to create an EDU.[47] In November 2023, Ursula von der Leyen, in her speech at the European Defence Agency's annual conference, reiterated again that the EU needs to become a full-fledged EDU. Accordingly, the European Commission began to develop a European Defence Industrial Strategy (EDIS), which was accepted in March 2024.[48]

43 Fiott, 2020, p. 7.
44 European Commission, 2021.
45 von der Leyen, 2021.
46 Consilium, 2022.
47 European Commission, 2023a.
48 EDA, 2023.

5. The current situation of new initiatives

The acceptance of the EU Global Strategy in 2016 can be considered a turning point in the CSDP development process. Since 2016, this process has been built on at least seven pillars:

1. establishment of the Military Planning and Conduct Capability (MPCC);
2. introduction of the Coordinated Annual Review on Defence (CARD);
3. establishment of the Permanent Structured Cooperation (PESCO);
4. creation of the European Defence Fund (EDF);
5. establishment of the European Peace Facility (EPF);
6. development of Rapid Deployment Capacity (RDC);
7. regulations on Common Procurement.

It is worth mentioning that the MPCC created a permanent command structure for EU (non-executive) military operations. With the creation of EDF, it became possible to fund research and joint development defence projects from the EU budget, which allowed for the provision of weapons to third countries involved in military operations for the first time. These achievements were unimaginable a decade ago.

The deteriorating security situation in Europe, created by Russian aggression in Ukraine, led to the strengthening of the military aspects of the Union. Military equipment was provided to Ukraine through EPF. Therefore, the available amount increased significantly. Approximately 60,000 Ukrainian soldiers were trained by the EU Military Assistance Mission as of the end of 2024. In 2022, in the shadow of the war, the EU adopted its first-ever military concept, the Strategic Compass. This document highlights the need to create strategic autonomy and technological sovereignty.[49]

6. The main pillars of closer defence integration/building blocks of EDU

Military Planning and Conduct Capacity – MPCC

The establishment of MPCC in 2017 was one of the pillars for closer defence cooperation. It can be considered the basis for a permanent military command structure in the EU. Since 2017, the MPCC, established within the EU Military Staff, has provided permanent strategic command to non-executive military missions. It holds command of the EU Training Missions (EUTM), currently in operation in Mali, Central African Republic, Somalia, Mozambique and Ukraine.[50]

49 European External Action Service, 2022.
50 Consilium, 2017a; European Parliament, 2016c; Howorth, 2017; Reykers, 2019.

In November 2018, the Council decided to strengthen the staff and responsibilities of the MPCC. According to the decisions of Member States, by the end of 2020, the MPCC should have been ready to provide permanent operational planning and build a structure to command and control an executive military CSDP operation.[51] In April 2019, the EEAS prepared a concept regarding further development of the MPCC for the EU Military Committee, detailing the planned command and control structure.[52] Negotiations on new tasks of MPCC continued in the following years.[53]

The MPCC has been responsible for the operational planning and conduct of non-executive military missions (EUTM) in Mali, Somalia, the Central African Republic, and Mozambique, and the EU Military Assistance Mission (EUMAM) for Ukraine. It was established to further increase civilian and military cooperation, as it works in close cooperation with the Civilian Planning and Conduct Capability through the Joint Support Coordination Cell at a strategic level. The MPCC reports to PSC, which provides political control and strategic direction for CSDP military operations and informs the EUMC. The Director General of the EU Military Staff plays a dual role; he is the Director of the MPCC as well as the Mission Commander for all non-executive military missions.[54]

The EU Strategic Compass (2022) describes the MPCC as the preferred military strategic level C2 structure:

> Military Planning and Conduct Capability is fully able to plan, control, and command non-executive and executive tasks and operations, as well as live exercises. In this context, we will ramp up personnel contributions and ensure that we have the necessary communication and information systems, as well as required facilities. Once the Military Planning and Conduct Capability reaches its full operational capability, it should be seen as the preferred command and control structure. This will not affect our ability to continue using the pre-identified national operational Headquarters.[55]

In October 2023, the first live exercise (LIVEX 23) of the Rapid Deployment Capacity (RDC) was organised and led by MPCC.[56] According to these plans, all non-executive military missions, two small-scale or one medium-scale executive operation(s) and live exercises could be led by the MPCC command by 2025.[57]

51 Consilium, 2018.
52 Consilium, 2019.
53 Consilium, 2020b.
54 European External Action Service, 2023.
55 European External Action Service, 2022, p. 28.
56 Borrell, 2023.
57 European External Action Service, 2023.

6.1. Coordinated Annual Review on Defence – CARD

At the Council meeting in November 2016, the High Representative of the Union for Foreign Affairs and Security Policy presented an implementation plan for security and defence of Member States. It included 13 proposals to achieve the new strategic objectives laid down in the Global Strategy, including the CARD initiative.[58]

Contrary to the original idea of the "European Defence Semester" process (similar to the European Semester), Member States accepted a more flexible model based on voluntary consultations. The EDA, in cooperation with EEAS, developed elements of the review process. The EU Military Committee and competent authorities of Member States also discussed the policy document detailing CARD elements. Consequently, the final draft was prepared based on wide-ranging consultation. On 18 May 2017, the EU Council of the EU approved the rules for establishing CARD. The EDA, in cooperation with EU Military Staff, provided the CARD Secretariat. In 2018, the EDA led the first trial operation of CARD. The aim of the de facto two-year process is to provide a comprehensive overview of national defence planning and development to address existing shortfalls, identify opportunities for further cooperation and ensure the coherence and optimal use of defence spending. Recommendations are detailed in the final report, presented to defence ministers.[59]

Following the first CARD cycle between 2019 and 2020, the first full report was completed and presented to defence ministers in November 2020, providing an overview of the national defence planning and capability development efforts of 26 EDA Member States. The document recognised collaborative opportunities for Capability Development and Research & Technology.[60]

The second CARD cycle was realised between 2021 and 2022, following a bilateral dialogue between participating Member States and EDA regarding their defence characteristics and plans within the EU framework. Recommendations for further collaboration in European capability development were developed for individual Member States. The Ministers of Defence approved the second CARD Report in November 2022. The report found that the growth in Member States' defence spending because of Russian aggression against Ukraine can be considered both as a sad opportunity and a challenge for the EU.[61]

6.2. Permanent structured cooperation – PESCO

One of the most important innovations of the Lisbon Treaty was the extension of enhanced cooperation in the field of CSDP. The Treaty created a permanent structured cooperation as a new and flexible instrument to promote interoperability,

58 Jones, 2020.
59 EDA, 2016.
60 EDA, 2020.
61 EDA, 2022; EDA, no date.

reduce capability shortfalls and strengthen cooperation in the field of defence. The EU Treaty did not link the establishment of PESCO to a minimum number of Member States. Following the decision of Member States, the High Representative of the Union for Foreign Affairs and Security Policy gives an opinion on Member States' intentions. The EU Council makes the final decision based on a qualified majority. The European Parliament must be informed of this process. PESCO's development followed the German inclusive approach rather than the French exclusive approach.[62] After the decision of Member States, in December 2017, the EU Council decided, by a qualified majority, to launch PESCO with the participation of 25 countries. Denmark, the United Kingdom and Malta decided not to take part in the new initiative. In June 2022, Denmark joined CSDP following a successful referendum abolishing the opt-out on European defence cooperation. In March 2023, the Danish Parliament voted in favour of the country's participation in PESCO and EDA. The Foreign Affairs Council (with defence ministers) voted for Denmark's participation in PESCO at a meeting on 23 May 2023.[63]

The EEAS and EDA jointly provide for the PESCO Secretariat. One of the main tasks of EDA is to formulate proposals based on the CARD to achieve the goals of the Capability Development Plan. Compared with the previous activities of EDA, the significance of PESCO is demonstrated by the fact that the commitments of Member States regarding the projects have become accountable.[64]

Following these five waves, 68 PESCO projects are currently ongoing. PESCO has developed a two-level governance system. On the one hand, there are common rules, and on the other, participating Member States decide the details of each project. The fact that PESCO projects can receive additional funding from EDF makes cooperation sustainable. However, the success of PESCO projects primarily depends on the political will of participating Member States,[65] as it has received criticism regarding its implementation.[66]

6.3. European Defence Fund – EDF

In September 2016, President of the European Commission Jean-Claude Juncker announced the establishment of EDF. As part of the EU Global Strategy implementation process, the European Commission presented EDAP in November, which already contained concrete proposals for the creation of the fund. The European Commission started testing the EU-level defence cooperation with the Preparatory Action on Defence Research programme between 2017 and 2019 and the European Defence Industrial Development Programme between 2019 and 2020.

62 Fiott, Missiroli and Tardy, 2017.
63 Danish Ministry of Defence, 2023.
64 Molnár, 2018; Molnár, 2019; Consilium, 2017b.
65 Biscop, 2020.
66 Blockmans and Macchiarini-Crosson, 2019.

According to the European Commission's initial proposal, the new fund provided 90 million euros per year between 2017 and 2019 during the testing period of the mechanism and around 500 million euros per year for the budget period 2021–2027 to support the defence industry. This fund was intended to complement the national resources available for defence research, procurement and prototype development. The novelty of this programme was that, for the first time, it became possible to use EU budget resources for the development of the defence industry. The legal basis for establishing EDF is Articles 173 and 182 of the Treaty on the Functioning of the EU (TFEU). According to Article 173, 'the Union and Member States shall ensure that the conditions necessary for the competitiveness of the Union's industry exist.'

In June 2018, the European Commission announced a proposal for a multiannual financial framework between 2021 and 2027. The Commission planned to enhance EDF's budget to 13 billion euros to boost EU-SA and its global role. The fund, which co-finances projects with a minimum of three participants from at least three Member States, aims to serve as a catalyst to build an innovative and competitive industrial and scientific base and strengthen small and medium enterprises. Collaborative projects realised under PESCO can receive an additional 10% co-financing from the fund. After heated debates, in December 2020, the Council adopted and the European Parliament consented to the EU's multiannual financial framework for 2021–2027. The EDF received a budget of 7.9 billion euros.[67]

6.4. European Peace Facility – EPF

In 2018, the High Representative for Foreign Affairs and Security Policy presented a proposal to create a 10.5 billion-euro instrument, the European Peace Facility (EPF). The new off-budget financial instrument became part of the EU's crisis management toolbox. It aims to make the EU 'a more efficient and responsive global security provider'. The new instrument replaced the African Peace Facility and the Athena Mechanism and was funded by Member States' annual gross national income-based contributions. The budget is available for the Common Costs of CSDP military operations and Assistance Measures in support of third countries or international organisations. According to the original targets, 35–45% of the operational costs of military operations should be covered by this fund. In addition, it allows financial support for partner countries in Africa and EU neighbourhoods to strengthen their resilience.[68] It is planned to facilitate rapid deployment outside the EU and support flexibility.[69] The EPF has made it easier to finance CSDP military missions.

In December 2020, the EU Council reached a political agreement to utilize EPF to finance military- or defence-related external activities. Compared to the original proposal, the new instrument could count on much less – only five billion euros

67 Consilium, 2020a.
68 Deneckere, 2019; European External Action Service, 2018.
69 Puig-Soler, 2021.

– between 2021 and 2027. The EPF, together with the Neighbourhood, Development and International Cooperation Instrument, supports partner countries in prevention and management of crises, and strengthening their resilience.

Russian invasion of Ukraine in 2022, triggering a deteriorating security environment, set the EPF in motion. Accordingly, the total budget increased, reaching more than 17 billion euros between 2021 and 2027. This has become one of the most important tools for Ukraine to defend its territorial integrity and protect its citizens from Russian aggression. In the framework of EPF, 5.6 billion euros was mobilised for the military support of Ukraine.[70] In March 2024, the Council of the EU decided to increase the financial resources of EPF by 5 billion euros and secure support for Ukraine by creating the Ukraine Assistance Fund inside the EPF.[71] It is worth mentioning that the flexible decision-making tool of constructive abstention was used by neutral countries (Austria, Malta and Ireland) and by Hungary during decisions regarding EPF.

6.5. EU Rapid Deployment Capacity – RDC

As mentioned previously, EU BGs have never been deployed and there have been serious doubts about their applicability. A large body of literature highlights the problems surrounding BGs.[72] The main obstacles to their deployment are the lack of political will and substantial funding opportunities of Member States. It is no coincidence that the idea of extending the Athena Mechanism to this area has been discussed as well. This process also entailed rethinking the entire financial system. Consequently, in 2021, the EPF succeeded the Athena Mechanism and African Peace Facility.

In 2021, 14 EU Defence Ministers (Austria, Belgium, Cyprus, the Czech Republic, Germany, Greece, France, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Slovenia, and Spain) asked Josep Borrell (HR/VP) to establish a new rapid military response capacity (called First Entry Force) for crisis management outside the EU.[73]

The Strategic Compass (2022) indicated the creation of an EU Rapid Deployment Capacity (RDC). According to the EU's first-ever military strategy, an RDC will be fully operational and swiftly deployable by 2025. EU Member States decided to agree on operational scenarios in 2022 and organise the first live exercises in 2023. The Compass declared that the RDC 'will consist of substantially modified EU BGs and pre-identified Member States' military forces and capabilities'.[74]

Although EUBGs are considered the building blocks for RDC, there are major differences between them. In opposition to EUBGs, the RDC will be a modular force of

70 European Commission, 2023b; European Commission, 2023c.
71 Council of the European Union, 2024.
72 Balossi-Restelli, 2011; Reykers, 2017; Ringsmose and Rynning, 2017; Tsitsikostas, 2021; Meyer, Van Osch and Reykers, 2022.
73 Barbosa-Lobo, 2021; Meyer, Van Osch and Reykers, 2022, p. 4.
74 European External Action Service, 2022.

5,000 troops, including land, air and maritime elements, and strategic enablers (such as cyber-defence, satellite communications, intelligence, surveillance and reconnaissance capabilities).[75] Another difference between the two is the length of the rotation period. Currently, it is panned to extend the six months to one year.

According to Meyer, Van Osch and Reykers, the EU RDC cannot be considered a 'single force of 5,000 troops but rather as a toolbox of force packages with land, air and maritime components, plus strategic enablers (such as strategic airlift and intelligence for target acquisition)'. This means that EUBGs are supposed to be substantially modified 'in line with the single set of forces principle'.[76]

Since the beginning, it has been planned that MPCC will provide C2 capacities for live exercise and the first RDC. In October 2023, the first live exercise (LIVEX 23) of RDC was conducted in Cadiz (Spain) under the control of the MPCC.[77]

6.6. Regulations on Common Procurement

The Russian invasion of Ukraine in 2022 highlighted the weaknesses of the European defence industry in terms of fragmentation and underfunding. On 11 March 2022 at their informal meeting in Versailles, members of the European Council committed themselves to strengthening the European defence technological and industrial basis and requested that the European Commission continue planning in the policy area.[78]

The war in Ukraine posed a great challenge to the European defence industry, which was undersized and faced problems. In the wake of increasing demand and shortage of assets leading to procurement from outside the EU, and hindering the attainment of the European objectives concerning the European defence technological and industrial base, in July 2022, the European Commission proposed two legal incentives to procure defence products jointly: in the short term, the approval of the "European Defence Industry Reinforcement through Common Procurement Act" (EDIRPA), and in the long term, the EDIP. Owing to increased demand, on 3 May 2023, the EC submitted another proposal for adopting the Regulation on Establishing the Act in Support of Ammunition Production (ASAP). After reaching a political agreement, the European Parliament and the Council adopted the ASAP regulation, which was published in the Official Journal of the EU on 20 July 2023. This new regulation complements EDIRPA.[79] The purpose of ASAP is to support an increase in the ammunition and missile production capacity of the EU in the interest of Ukraine and EU Member States. The European Parliament and the Council adopted the EDIRPA Regulation in the autumn of 2023. The new regulation was published in the Official

75 Zandee and Stoetman, 2022, p. 2.
76 Meyer, Van Osch and Reykers, 2022, p. 4.
77 Borrell, 2023.
78 Consilium, 2022.
79 *Regulation (EU) 2023/1525 of the European Parliament and of the Council of 20 July 2023 on supporting ammunition production (ASAP)*, 2023.

Journal of the EU on 26 October 2023, and entered into force the day following its publication.[80] After the State of the Union address of President von der Leyen in 2023, the EC initiated a consultation process to develop a new EDIS, which was published in March 2024.

7. Mapping national defence policies regarding European strategic autonomy

As the concept of EDU is promoted mainly by EU Institutions and is not mentioned in Member States' strategic documents, the aim of this subchapter is to analyse Member States' views on the concept of EU-SA. This part of the research is based on an assessment of secondary literature and analysis of the latest national security strategic documents, particularly the national security strategies of Member States.

Within the EU, there are several traditional clusters promoting defence cooperation (i.e. the Franco–German alliance, Weimar Triangle, Benelux countries,[81] NORDEFCO,[82] V4 countries and Baltic countries[83]). Among them, the Franco–German axis is perhaps the most significant. It was originally established by the 1963 Elysée Treaty and reinforced by the 2019 Aachen Treaty.[84] In 2021, Italy and France created a similar alliance, signing the Quirinal Treaty for Strategic Relationships that came into force on 1 February 2023.[85] France, Italy and Spain, along with Germany are considered the "defence frontrunners" in Europe.[86] These countries are involved in most of the EDF and PESCO projects. Originally, the so-called Four Big European countries were France, Germany, Italy and the United Kingdom; however, after Brexit, Spain could be considered one of the four big countries that intended to play a decisive role in the development of defence integration in Europe. This is demonstrated by the fact that in 2020, the Ministers of Defence in France, Germany, Italy and Spain proposed starting the elaboration of the *Strategic Compass*, beginning the process with a threat analysis.[87]

80 *Regulation (EU) 2023/2418 of the European Parliament and of the Council of 18 October 2023 on establishing an instrument for the reinforcement of the European defence industry through common procurement (EDIRPA)*, 2023.
81 Meijer and Wyss, 2018.
82 See: https://www.nordefco.org/the-basics-about-nordefco (Accessed: 21 June 2024).
83 Republic of Estonia, Ministry of Defence, 2015.
84 French Ministry for Europe and Foreign Affairs, 2019.
85 Governo Italiano, 2021.
86 Blockmans, 2021.
87 Zandee et al., 2020, p. 24.

Among the Big Four countries, French President Macron has become the most important political supporter of EU-SA and European sovereignty. France has historically backed the idea of EU-SA to reduce dependence of Europe since the late 1990s.[88] The last revision of the French NSS occurred in 2022, triggered by the Russian aggression. The promotion of EU-SA is one of the ten priorities of the French National Strategic Review. The document indicates that the defence of French security interests 'is built on three pillars, that is, strengthening of strategic autonomy; attaining European sovereignty and consolidation of alliances; and preservation of a stable international order based on respect for the law and multilateralism'.[89] According to strategic objectives of the document, France intends to be the driving force behind EU-SA.[90]

Germany has adopted its first comprehensive NSS in 2023 (Robust. Resilient. Comprehensive. Integrated Security for Germany). According to the strategy, European integration was first viewed as a peace project. Although the text does not explicitly mention EU-SA or sovereignty, it claims that strengthening the EU's ability to act is one of the main interests of Germany. Germany wants to strengthen the European pillar of NATO, further develop CFSP and implement the Strategic Compass. The CSDP is an important tool for crisis management outside of the EU. Although NATO is considered the primary guarantor of protection against military threats, the text claims that Germany's commitments not only to NATO but also to the EU's mutual assistance clause (Article 42(7) TEU) are unshakeable.[91]

Despite the presence of various official documents related to security and defence, Italy does not have a NSS. The White Paper on International Security and Defence from 2015 can be interpreted as a type of NSS. The Italian Ministry of Defence publishes the Multi-Year Defence Planning Document (Documento Programmatico Pluriennale, DPP) annually. This annual decree can also be considered a short-term strategic document for Italian security and defence policy. The current document for 2023–2025 highlights Italy's support for NATO as an organisation guaranteeing the security of the Euro–Atlantic space. Simultaneously, it emphasises that Italy will strengthen its contribution to the initiatives and operations of the EU CSDP, supporting its ambition of growing strategic autonomy.[92] Although the Trans-Atlantic relationship is extremely important for Italy, its government supported it and played a decisive role in the elaboration of the EU GS under the work of Federica Mogherini as former HR/VP. The EU-SA is seen in the country as a complementary tool for national- end European security and not as a tool for reducing dependence on Trans-Atlantic relations.[93]

88 Libek, 2019.
89 République Française, 2022, p. 19.
90 République Française, 2022, p. 27.
91 Federal Government of Germany, 2023, p. 31.
92 Governo Italiano, Ministero della Difesa, 2023, p. 16.
93 Zandee et al., 2020, p. 38.

Spain elaborated on its latest NSS in 2021. According to this document, Spain has a more comprehensive view of the EU-SA. As stated in the document,

> Spain is committed to greater European strategic autonomy, combining the promotion of the CSDP and the area of freedom, security and justice with the improvement of health security progress in energy union or the greater role of the European Union in the management of cross-border crises are also part of the broad spectrum of policies aimed at strengthening European security and the role of the Union as a global actor.[94]

It is no coincidence that Spain, along with the Netherlands, published a non-paper on EU-SA, which claimed that it is important to combine an open economy with the reduction of some strategic dependences to avoid protectionism. The document promotes the concept of open strategic autonomy (OSA).[95] In 2023, the Spanish Presidency of the Council of the EU prepared a non-paper in close consultation with the 27 Member States and EU institutions to contribute to the development of 'a comprehensive, balanced and forward-looking approach to ensure OSA and global leadership by 2030'.[96] It is important to highlight that the Spanish presidency identifies OSA as a tool for reindustrialisation of Europe, and not as a tool exclusively for CSDP.[97] OSA aims to guarantee that:

> the EU has the capacity to cope alone if necessary but without ruling out cooperation whenever possible. It goes some steps beyond smart supply chain management by taking into account geopolitics as well as economic factors. It relies on foresight to identify threats and ensures resilience by anticipating the required responses.[98]

Since 1991, France and Germany have cooperated with Poland within the framework of the Weimar Triangle (WT). Although the creation of "Weimar Plus" was proposed by the foreign and defence ministers of Spain and Italy in 2012, this form of cooperation has not been developed.[99] Within the WT, Poland's Atlanticist views affected diplomatic relations among the three countries. Following the Polish parliamentary elections of 2015, which resulted in the victory of Law and Justice (PiS), Poland played a more active role in V4 cooperation. This is illustrated by the fact that no WT foreign minister meetings took place between 2016 and 2020.[100] The joint declaration issued in January 2020 did not refer to foreign, security or

94 Presidencia del Gobierno, 2021.
95 Kingdom of the Netherlands, 2021.
96 Spain's National Office of Foresight and Strategy, 2023.
97 Orłowski, 2023.
98 García-Higuera and Weichert, 2023.
99 Ministère de l'Europe et des Affaires Étrangères, 2024.
100 Federal Foreign Office, no date.

defence policies.[101] As a consequence of dynamic economic growth and military developments, Poland can be considered an emerging European power. Owing to Russian aggression in Ukraine, cooperation within the WT gained impetus. At the WT Summits in 2022, 2023 and 2024, leaders of the three countries expressed solidarity with Ukraine. In a joint press release in 2023, the leaders expressed their commitment to continue the implementation of the Versailles Declaration and the Strategic Compass, focusing on strengthening the European defence technological and industrial base, and reinforcing the complementarity between European defence and NATO.[102] Despite the strengthened cooperation within WT, the previous Polish government criticised the concept of EU-SA and instead proposed a strategic partnership between the EU and the United States.[103] In February 2024, the Joint Statement of WT Foreign Ministers stated that:

> extraordinary times require extraordinary measures. Against this background, it is our goal to make the European Union more united, stronger and able to respond to today's security challenges, on a path towards a security and defence union, living up to our citizen's expectations. We are also committed to a strong and united NATO.[104]

Until now, not only Spain and Poland but also the Netherlands, East–Central Europe, Baltic and Scandinavian countries, and Portugal have criticised the concept of EU-SA or European Sovereignty. Several Member States have been distrustful of the concept of the potential promotion of protectionism, and have been wary of undermining the Transatlantic alliance and NATO. Therefore, the Member States have proposed the concept of OSA.[105]

In 2021, 12 EU Member States – led by Denmark and consisting of Sweden, Finland, the Netherlands, Ireland, Lithuania, Latvia, Estonia, the Czech Republic, Slovakia, Malta and Spain – prepared a joint non-paper on OSA, emphasising the importance of the EU's openness to trade and investment.[106]

Belgium, Finland, the Netherlands, Portugal and Slovakia prepared another joint non-paper about OSA in 2023, highlighting that:

> a geopolitically fragmented world demands a strong and resilient Union that is able to safeguard and promote its core interests, strive for a rules-based, open, and interconnected economy and champion multilateralism and international cooperation.

The concept of OSA was introduced to achieve just that.

101 French Ministry for Europe and Foreign Affairs, 2019.
102 Élisée, 2023.
103 Besch and Varma, 2023.
104 Ministère de l'Europe et des Affaires Étrangères, 2024.
105 Torreblanca and Jorge-Ricart, 2022, pp. 3, 17.
106 Van den Abeele, 2021, p. 21.

It also declared that the EU and NATO should be mutually reinforced and cooperation between the two organisations should be deepened.[107]

Although Benelux countries have traditionally supported deepening integration in the field of CSDP, they have also supported the concept of OSA. According to the Dutch security strategy, the Netherlands aims to strengthen the EU's open strategic autonomy policy to reduce strategic dependence. The document underlines that, within the EU context, strengthening CSDP, as outlined in the EU Strategic Compass, will also help strengthen NATO.[108] Belgium has developed its first NSS in 2022. Regarding the concept of the EU-SA, the document underlines that there is no consensus on the concept of autonomy and highlights the importance of OSA, which does not lead to protectionism.[109] According to Luxemburg's latest defence guidelines, the achievement of EU-SA in defence issues while promoting EU–NATO cooperation represents a major challenge. Being members of both organisations, it is challenging to avoid duplication.[110]

Scandinavian Members of the EU have traditionally criticised the concept of EU-SA. Denmark used to hold a special position within the EU, which was attributed to its national opt-out on CSDP. Having a dominantly Atlanticist view, the country intensely contested the idea of EU-SA. Finland originally had an ambiguous opinion of EU-SA. While strongly supporting the EU in becoming a global player and security provider, it insisted on the importance of involving non-EU partners in the realisation of CSDP. Finland also supported the concept of OSA.[111] As Sweden has also been concerned about the weakening of Transatlantic relations, it expressed a critical opinion about the EU-SA, as the maintenance of global free-trade rules represents common interests for Scandinavian countries.[112] Russian aggression in Ukraine has had a significant impact on the security and defence policies of Scandinavian Member States, considering that in 2022, Sweden and Finland decided to leave behind neutrality, and both countries are now members of the NATO. Denmark also made historic decisions. At the successful referendum on 1 June 2022, voters backed Denmark's participation in all elements of the EU's CSDP by abolishing the Danish opt-out on defence. Consequently, Denmark decided to contribute to military operations ALTHEA in Bosnia and Herzegovina in December 2022, and to the EU's EUMAM.[113] The most recent Danish foreign and security policy strategy was published in May 2023. The document emphasised that Denmark intends to achieve strengthened resilience through closer European cooperation. Countries require an EU that can act quickly and decisively. Denmark is committed to strengthening its EU position through OSA.[114] Swe-

107 Kingdom of the Netherlands, 2023.
108 Government of the Netherlands, 2023, pp. 22, 30.
109 Kingdom of Belgium, 2022, p. 31.
110 Government of the Grand Duchy of Luxembourg, 2023, p. 66.
111 Torreblanca and Jorge-Ricart, 2022, pp. 3, 17.
112 Nissen, 2021, pp. 6–7.
113 Danish Ministry of Defence, 2023.
114 Ministry of Foreign Affairs of Denmark, 2023, p. 25.

den's latest NSS does not mention EU-SA, but emphasises the importance of a strong transatlantic link for Europe's security. According to this document 'the EU's role in security and defence needs to be strengthened in a way that favours transatlantic link without compromising the competence of Member States'.[115] In June 2023, the Swedish Defence Commission published its report on Sweden's Security Policy, emphasising that Sweden is best defended within NATO. NATO membership is vital for Sweden as well as for NATO, as it will strengthen security. Although the document does not mention EU-SA, it claims that the EU is Sweden's most important foreign policy arena. Sweden's responsibility towards EU Member States has also been highlighted. Article 42.7 TEU and the solidarity clause in Article 222 TEFU are important tools of joint responsibility for Europe's security. Nevertheless, NATO provides the foundation for the collective defence of its members.[116]

Within the EU, the Visegrad Four used to be considered a separate group, where, despite the different perceptions of security threats, defence ministers started to organise their regular meetings in 1999, and defence cooperation was strengthened in 2012.[117] The most significant example of cooperation in the field of defence was the establishment of V4 EU BGs. Owing to differing foreign policy goals and perceptions of Russian threats in Europe, the V4 group has gradually lost its significance.

The latest NSS of Poland emphasises the importance of a pragmatic approach to the development of CSDP (PESCO, EDF), ensuring its complementarity with NATO. EU-SA has not been mentioned in the strategy.[118] According to Czechia's NSS, the EU provides decisive contributions to its security in a broader sense. The EU's role as a strong political and security actor is mentioned as an interest of the country. Czechia supports efforts to reinforce the EU's CSDP while respecting the complementary approach to NATO's key role in collective defence. Czechia promotes the consistent growth of EU–NATO cooperation. The document also emphasises transatlantic relations.[119] The latest NSS of Hungary (2020) states that membership in NATO and the EU has substantially increased Hungarian security. Although the country maintains the primacy of NATO's collective defence, EU's role in the field of defence must be significantly strengthened. The document states that Hungary is interested in increasing the effectiveness of EU's CFSP and CSDP to complement the activities of NATO.[120] According to Slovakia's NSS, membership in NATO and the EU is the basic pillar of security of the Slovak Republic.[121] The concepts of EU-SA or OSA have not been mentioned in the latest national security strategies of V4 countries. It is worth

115 Government Office of Sweden, 2024, p. 29.
116 Swedish Ministry of Defence, 2023, pp. 4–5.
117 Visegrad Group, 2014.
118 National Security Bureau of the Republic of Poland, 2020, p. 24.
119 Ministry of Foreign Affairs of the Czech Republic, 2023, p. 21.
120 The Government of Hungary, 2021.
121 Slovak Republic, 2021, p. 5.

mentioning that the Czech Armaments Defence Industry Strategy (2022) mentions EU-SA.[122]

In this context, it is important to mention the Central European Defence Cooperation (CEDC), which was established in 2010, based on Hungarian and Austrian proposals. The CEDC group includes Austria, the Czech Republic, Croatia, Hungary, Slovakia and Slovenia (with Poland as an observer). This military cooperation aims to support EU's efforts towards European security.[123] The most recent comprehensive strategic document in Austria was published in 2013, underlining the EU role in security policies. The document states that Austria plays an active role in shaping CFSP and participates in the full spectrum of CSDP activities.[124]

EU countries in the Black Sea Region and the Western Balkans, like Romania or Croatia, which are also members of NATO, usually mention the EU as part of the foundation of their security without any reference to EU-SA or OSA, and in their strategic documents the complementarity with NATO is also emphasised.[125]

In Southern Europe, Portugal concluded a bilateral defence treaty with Spain in 2015.[126] Portugal published its latest Strategic Concept of National Defence in 2013, highlighting the importance of CSDP.[127] The revision of this document began in 2022, and the process has yet to be completed. In the Mediterranean region, Malta and Cyprus are not members of NATO. Malta followed the policy of neutrality and decided not to participate in PESCO. Cyprus represents a special category, as due to its territorial dispute with Turkey has a strong relationship with NATO.[128] Owing to the conflict between Turkey and Cyprus, cooperation between Greece and Cyprus was considered decisive. Since 2007, Cyprus has been a regular participant in Greek-led EU BGs. As NATO cannot be an option for Cyprus, it aimed to play a decisive role in the entire spectrum of CSDP.

The concept of EU-SA was originally associated with security and defence policies. Today, it has a much broader meaning, covering economic, technological and energy policies. Member States have developed different opinions on this concept. There were three groups of Member States. First, the NSSs of some countries have prioritised EU-SA, while others have developed the concept of OSA; in the documents of the third group, neither the EU-SA nor the OSA are integrated. The latter Member States have been confirmed by more Transatlanticists.

122 Ministry of Defence of the Czech Republic, 2022.
123 Honvédelmi Minisztérium, 2020.
124 Federal Chancellery of the Republic of Austria, 2013, p. 13.
125 Romania Presidential Administration, 2020; Republic of Croatia, 2017.
126 Branco, 2015.
127 República Portuguesa, 2013.
128 *Treaty no. 5476. United Kingdom of Great Britain and Northern Ireland, Greece and Turkey and Cyprus*, 1960.

8. Conclusions

CSDP is one of the youngest policy areas in the EU. Since its early phase, this field of integration has comprised not only the development of crisis management tools and institutional structures but also initiatives related to capability development processes. During the last decade, the security environment has deteriorated rapidly and external factors have had a significant impact on the accelerated integration process. Although in this policy area, intergovernmentalism remained the decisive form of decision-making processes within the European Council and the Council of the EU, Member States have decided unanimously on a number of initiatives inciting closer cooperation in the field of European defence. Today, the dynamics of the European integration process in the fields of CFSP and CSDP are defined by the duality between intergovernmentalism and supranationalism.

However, the hybrid power character of this international actor still provokes dispute. Significant changes have taken place in the international system: great power competition has intensified again. The rise of new powers has threatened the multilateral liberal global order and multilateralism. It is no coincidence that the EU had to adapt itself to major changes in international relations that led to a new arms race. EU-SA and EDU are key elements of this adaptation process for becoming a more autonomous actor in international relations and, thus, a real global player and security provider.

Since the adoption of GS (2016), Europe's security and defence cooperation has been accelerated by external factors. Following Russian aggression in Ukraine, the ideas of EU-SA and the EU became progressively relevant. These issues have gained increasing significance in recent years with armed conflicts (traditional and hybrid warfare) in the direct and wider neighbourhoods of the EU.

Member States have developed diverse opinions regarding EU-SA, which was originally associated with security and defence policy. Today, it has an extended meaning, including economic, technological, and energy policies. The NSS of one group of Member States mentions EU-SA as a priority, while another group has developed the concept of OSA; in the documents of a third group, neither EU-SA nor OSA have been mentioned. This last group of Members of State represents a more Transatlanticist perception of security and defence.

References

van den Abeele, É. (2021) 'Towards a new paradigm in open strategic autonomy?', *European Trade Union Institute aisbl*, Working Paper 2021.03. [Online]. Available at: https://www.etui.org/sites/default/files/2021-06/Towards%20a%20new%20paradigm%20in%20open%20strategic%20autonomy_2021.pdf (Accessed: 21 June 2024).

Aggestam, L. (2008) 'Introduction: Ethical Power Europe?', *International Affairs (Royal Institute of International Affairs 1944-)*, 84(1), pp. 1–11; https://doi.org/10.1111/j.1468-2346.2008.00685.x.

Balossi-Restelli, L.M. (2011) 'Fit for what? Towards explaining Battlegroup inaction', *European Security*, 20(2), pp. 155–184; https://doi.org/10.1080/09662839.2011.564767.

Barbosa-Lobo, R. (2021) 'EU in Talks to Develop First Entry Force', *Finabel*, 24 June 2021. [Online]. Available at: https://finabel.org/eu-in-talks-to-develop-first-entry-force/ (Accessed: 21 June 2024).

Besch, S., Varma, T. (2023) 'Biden Should Press Poland and the EU to Make Up. Warsaw's strategic role in Europe is too important for Washington to ignore', *Foreign Policy*, 22 September 2023. [Online]. Available at: https://foreignpolicy.com/2023/09/22/poland-election-germany-france-eu-us-biden-russia-military-strategy-deterrence-europe/ (Accessed: 21 June 2024).

Bifulco, R., Nato, A. (2020) 'The concept of sovereignty in the EU – past, present and the future', *RECONNECT Project*. [Online]. Available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ceba74f0&appId=PPGMS (Accessed: 21 June 2024).

Biscop, S. (2017) 'European Defence: What's in the CARDs for PESCO?', *Security Policy Brief*, 2019/91, pp. 1–6. [Online]. Available at: http://www.egmontinstitute.be/content/uploads/2017/10/SPB91-Biscop.pdf?type=pdf (Accessed: 21 June 2024).

Biscop, S. (2018) *European Strategy: New Future for an Old Power*. New York, NY: Routledge; https://doi.org/10.4324/9780429427442.

Biscop, S. (2020) 'Battalions to Brigades: The Future of European Defence', *Survival*, 62(5), pp. 105–118; https://doi.org/10.1080/00396338.2020.1819654.

Blockmans, S. (2017) 'Differentiation in CFSP: Potential and Limits', *Istituto Affari Internazionali*, 8 March. [Online]. Available at: https://www.iai.it/sites/default/files/eu60_5.pdf (Accessed: 21 June 2024).

Blockmans, S. (2021) 'PESCO's Microcosm of Differentiated Integration' in Douma, W., Eckes, Ch., Van Elsuwege, P., Kassoti, E., Ott, A., Wessel, R.A. (eds.) *The Evolving Nature of EU External Relations Law*. Berlin: Springer, pp. 163–176.

Blockmans, S., Macchiarini-Crosson, D. (2019) 'Differentiated integration within PESCO, Clusters and convergence in EU defence', *CEPS: Research Papers*, 2019/04. [Online]. Available at: https://www.ceps.eu/ceps-publications/differentiated-integration-within-pesco/ (Accessed: 21 June 2024).

Borrell, J. (2023) 'LIVEX, the first ever EU live military exercise', *European External Action Service*, 19 October 2023. [Online]. Available at: https://www.eeas.europa.eu/eeas/livex-first-ever-eu-live-military-exercise_en (Accessed: 21 June 2024).

Brack, N., Coman, R., Crespy, A. (2019) 'Sovereignty conflicts in the European Union', *Les Cahiers du Cevipol*, 2019/4 (N° 4), pp. 3–30; https://doi.org/10.3917/lcdc.194.0003.

Branco, C. (2015) 'Portugal and the CSDP' in Fiott, D. (ed.) *The Common Security and Defence Policy: National Perspectives*. Academia Press. Egmont Paper 79/2015, pp. 83–85.

Cîrlig, C.-C. (2015) 'European defence cooperation State of play and thoughts on an EU army', *European Parliamentary Research Service*, March 2015. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/551346/EPRS_BRI%282015%29551346_EN.pdf (Accessed: 21 June 2024).

Commission of the European Communities (2004) 'Commission Green Paper of 23 September 2004 on defence procurement' COM(2004) 608 final. [Online]. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/defence-procurement.html (Accessed: 21 June 2024).

Consilium (2003) 'Contribution from Dr Sylvia-Yvonne Kaufmann, member of the Convention 'Requirements for the Constitutional Treaty for a European Union capable of Peace'' CONV 681/03, Brussels, 11 April 2003. [Online]. Available at: https://data.consilium.europa.eu/doc/document/CV-681-2003-INIT/en/pdf (Accessed: 21 June 2024).

Consilium (2004) 'Headline Goal 2010: approved by General Affairs and External Relations Council on 17 May 2004'. [Online]. Available at: https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede110705headlinegoal2010_/sede110705headlinegoal2010_en.pdf (Accessed: 21 June 2024).

Consilium (2013) 'Conclusions – 19/20 December 2013' EUCO 217/13, Brussels, 20 December 2013. [Online]. Available at: https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/140245.pdf (Accessed: 21 June 2024).

Consilium (2017a) 'Concept Note: Operational Planning and Conduct Capabilities for CSDP Missions and Operations' (OR.en) 6881/17, Brussels, 6 March 2017. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-6881-2017-INIT/en/pdf (Accessed: 21 June 2024).

Consilium (2017b) 'Defence Cooperation: Council Establishes Permanent Structured Cooperation (PESCO), with 25 Member States Participating', 11 December 2017. [Online]. Available at: www.consilium.europa.eu/en/press/press-releases/2017/12/11/defence-cooperation-pesco-25-member-states-participating/# (Accessed: 21 June 2024).

Consilium (2018) 'Security and Defence: Council welcomes the substantive progress made during the last two years' *Press Release*, 19 November 2018. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/security-and-defence-council-welcomes-the-substantive-progress-made-during-the-last-two-years/ (Accessed: 21 June 2024).

Consilium (2019) 'EU Concept for Military Command and Control – Rev 8' EEAS(2019) 468, Brussels, 23 April 2019. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-8798-2019-INIT/en/pdf (Accessed: 21 June 2024).

Consilium (2020a) 'Az EU 2021–2027-es időszakra vonatkozó hosszú távú költségvetése és a helyreállítási csomag' [EU long-term budget 2021-2027 and recovery package], 17 December 2020. [Online]. Available at: https://www.consilium.europa.eu/hu/policies/the-eu-budget/long-term-eu-budget-2021-2027/ (Accessed: 21 June 2024).

Consilium (2020b) 'List of Working papers (WK) distributed to the European Union Military Committee in the second quarter of 2020' Brussels, 17 July 2020. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-9586-2020-INIT/en/pdf (Accessed: 21 June 2024).

Consilium (2022) 'Informal meeting of the Heads of State or Government. Versailles Declaration' Versailles, 10 and 11 March 2022. [Online]. Available at: https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf (Accessed: 21 June 2024).

Council of the European Union (2004) 'COUNCIL JOINT ACTION 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency' OJ L 245, 12 April 2008. [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2004E0551:20080407:EN:PDF (Accessed: 21 June 2024).

Council of the European Union (2022) 'A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security' (OR. en) 7371/22, Brussels, 21 March 2022. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf (Accessed: 21 June 2024).

Council of the European Union (2024) 'Ukraine Assistance Fund: Council allocates €5 billion under the European Peace Facility to support Ukraine militarily' *Press Release*, 18 March 2024. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2024/03/18/ukraine-assistance-fund-council-allocates-5-billion-under-the-european-peace-facility-to-support-ukraine-militarily/ (Accessed: 21 June 2024).

Cross, M. (2011) 'Europe, a smart power?', *International Politics*, 2011/48, pp. 691–706; https://doi.org/10.1057/ip.2011.28.

Danish Ministry of Defence (2023) 'Denmark and the EU', 20 November 2023. [Online]. Available at: https://www.fmn.dk/en/topics/international-cooperation/eu/ (Accessed: 21 June 2024).

Deneckere, M. (2019) 'The uncharted path towards a European Peace Facility', *ECDPM Discussion Paper*, No. 248, 18 March 2019. [Online]. Available at: https://ecdpm.org/publications/uncharted-path-towards-european-peace-facility/ (Accessed: 21 June 2024).

Duchêne, F. (1972) 'Europe's Role in World Peace' in Mayne, R.J. (ed.) *Europe Tomorrow. Sixteen Europeans Look Ahead*. London: Collins, pp. 32–47.

Duchêne, F. (1973) 'The European Community and the Uncertainties of Interdependence' in Kohnstamm, M., Hager, W. (eds.) *A Nation Writ Large? Foreign-Policy Problems before the European Community*. London: Macmillan. pp. 1–21; https://doi.org/10.1007/978-1-349-01826-0_1.

EDA (2016) 'Coordinated Annual Review on Defence (CARD)', November 2016. [Online]. Available at: https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card) (Accessed: 21 June 2024).

EDA (2020) 'CARD Report 2020. Executive Summary' Brussels, November 2020. [Online]. Available at: https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf (Accessed: 21 June 2024).

EDA (2022) 'Coordinated Annual Review on Defence Report' Brussels, November 2022. [Online]. Available at: https://eda.europa.eu/docs/default-source/eda-publications/2022-card-report.pdf (Accessed: 21 June 2024).

EDA (2023) 'President von der Leyen unveils plans for defence strategy at EDA conference' *EDA Latest News*, 30 November 2023. [Online]. Available at: https://eda.europa.eu/news-and-events/news/2023/11/30/president-von-der-leyen-unveils-plans-for-defence-industrial-strategy-at-eda-conference (Accessed: 21 June 2024).

EDA (no date) 'Coordinated Annual Review on Defence'. [Online]. Available at: https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card) (Accessed: 21 June 2024).

Élisée (2023) 'Joint press release by the leaders of the Weimar Triangle', 24 February 2023. [Online]. Available at: https://www.elysee.fr/en/emmanuel-macron/2023/02/24/joint-press-release-by-the-leaders-of-the-weimar-triangle (Accessed: 21 June 2024).

European Commission (2017) 'Reflection Paper on the Future of European Defence' COM(2017) 315, 7 June. [Online]. Available at: https://commission.europa.eu/document/download/172d0a7c-161c-450b-b7f6-2d36acd7861f_en?filename=reflection-paper-defence_en.pdf (Accessed: 21 June 2024).

European Commission (2019) 'Towards a European Defence Union. Towards a More United, Stronger and More Democratic Union' *Publications Office*, May 2019. [Online]. Available at: https://op.europa.eu/en/publication-detail/-/publication/7e0c92fe-8e4d-11e9-9369-01aa75ed71a1 (Accessed: 21 June 2024).

European Commission (2021) 'Towards a European Defence Union. Towards a More United, Stronger and More Democratic Union', 30 January 2021. [Online]. Available at: https://ec.europa.eu/info/sites/info/files/towards-a-european-defence-union_en.pdf (Accessed: 21 June 2024).

European Commission (2023a) '2023 State of the Union Address by President von der Leyen'. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/ov/speech_23_4426 (Accessed: 21 June 2024).

European Commission (2023b) 'European Peace Facility'. [Online]. Available at: https://fpi.ec.europa.eu/what-we-do/european-peace-facility_en (Accessed: 21 June 2024).

European Commission (2023c) 'EU solidarity with Ukraine'. [Online]. Available at: https://eu-solidarity-ukraine.ec.europa.eu/eu-assistance-ukraine_en#support-for-military-equipment-and-training (Accessed: 21 June 2024).

European External Action Service (2016a) 'Speech by Federica Mogherini at the public seminar "EU as a Global Actor" Stockholm, 10 October 2016. [Online]. Retrieved from: https://eeas.europa.eu/headquarters/headquarters-homepage/11588/speech-by-federica-mogherini-at-the-public-seminar-eu-as-a-global-actor_en (Accessed: 21 June 2024).

European External Action Service (2016b) 'Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy' Brussels, 2 June. [Online]. Available at: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (Accessed: 21 June 2024).

European External Action Service (2018) 'European Peace Facility – An EU off-budget fund to build peace and strengthen international security' *EEAS Strategic Communications*, 13 June. [Online]. Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/46285/european-peace-facility-eu-budget-fund-build-peace-and-strengthen-international-security_en (Accessed: 21 June 2024).

European External Action Service (2022) 'A Strategic Compass for Security and Defence' *EEAS Strategic Communications*, 24 March. [Online]. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en (Accessed: 21 June 2024).

European External Action Service (2023) 'The Military Planning and Conduct Capability', February 2023. [Online]. Available at: https://www.eeas.europa.eu/sites/default/files/documents/2023/20230222_MPCC%20Factsheet.pdf (Accessed: 21 June 2024).

European Parliament (2016a) 'Next step in mutual defence – European Defence Union, say MEPs', 21 January 2016. [Online]. Available at: https://www.europarl.europa.eu/news/hu/press-room/20160114IPR09904/next-step-in-mutual-defence-european-defence-union-say-meps (Accessed: 21 June 2024).

European Parliament (2016b) 'European Parliament resolution of 22 November 2016 on the European Defence Union (2016/2052(INI))' *Official Journal of the European Union*, C 224/18, 27 June. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016IP0435 (Accessed: 21 June 2024).

European Parliament (2016c) 'Europe as a stronger global actor, European Defence Union' *Legislative Train Schedule*, 20 October 2016. [Online]. Available at: https://www.europarl.europa.eu/legislative-train/carriage/european-defence-union/report?sid=301 (Accessed: 21 June 2024).

European Parliament (2018) 'Report on differentiated integration' *Committee on Constitutional Affairs in the European Parliament*, (2018/2093(INI)). [Online]. Available at: https://www.europarl.europa.eu/doceo/document/A-8-2018-0402_EN.pdf (Accessed: 21 June 2024).

European Parliament (2022) 'EU strategic autonomy 2013-2023: From concept to capacity' *EU Strategic Autonomy Monitor,* July 2022. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf (Accessed: 21 June 2024).

European Parliament, Directorate-General for External Policies (2013) *The Development of a European Defence Technological and Industrial Base (EDTIB)*. Luxemburg: Publication Office; https://doi.org/10.2861/15836. Authored by: Briani, V., Marrone, A., Mölling, C., Valasek, T.

Federal Chancellery of the Republic of Austria (2013) 'Austrian Security Strategy Security in a new decade – Shaping security.' Vienna, July 2013. [Online]. Available at: https://www.bmlv.gv.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf (Accessed: 21 June 2024).

Federal Foreign Office (no date) 'The Weimar Triangle: Over 30 years of cross-border cooperation between Germany, France and Poland'. [Online]. Available at: https://www.auswaertiges-amt.de/en/aussenpolitik/europa/zusammenarbeit-staaten/-/228752 (Accessed: 21 June 2024).

Federal Government of Germany (2023) 'Robust. Resilient. Sustainable. Integrated Security for Germany. National Security Strategy.' *Federal Foreign Office*, June 2023. [Online]. Available at: https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf (Accessed: 21 June 2024).

Fiott, D. (2018) 'Strategic autonomy: towards 'European sovereignty' in defence?', *European Union Institute for Security Studies: Brief Issue*, 2018/12. [Online]. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2012__Strategic%20Autonomy.pdf (Accessed: 21 June 2024).

Fiott, D. (2020) 'Uncharted Territory? Towards a common threat analysis and a Strategic Compass for EU security and defence', *European Union Institute for Security Studies: Publications Office*; https://doi.org/10.2815/362443.

Fiott, D., Missiroli, A., Tardy, T. (2017) 'Permanent Structured Cooperation: What's in a Name?', *Chaillot Paper*, No. 142, Paris: EUISS. [Online]. Available at: https://www.iss.europa.eu/content/permanent-structured-cooperation-what%E2%80%99s-name (Accessed: 21 June 2024).

French Ministry for Europe and Foreign Affairs (2019) 'Franco-German Treaty of Aachen', 22 January 2019. [Online]. Available at: https://www.diplomatie.gouv.fr/en/country-files/germany/france-and-germany/franco-german-treaty-of-aachen/ (Accessed: 21 June 2024).

García-Higuera, A., Weichert, C. (2023) 'What if open strategic autonomy could break the cycle of recurring crises?', *European Parliamentary Research Service*, May 2023. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747420/EPRS_ATA(2023)747420_EN.pdf (Accessed: 21 June 2024).

Government of the Grand Duchy of Luxembourg (2023) 'Luxembourg defence Guidelines 2023' *Ministry of Foreign and European Affairs, Directorate of Defence*. [Online]. Available at: https://gouvernement.lu/dam-assets/documents/actualites/2023/05-mai/11-guidelines-defence/luxembourg-defence-guidelines-2035-en.pdf (Accessed: 21 June 2024).

The Government of Hungary (2021) 'Government Resolution 1163/2020 (21st April) on Hungary's National Strategy' *Magyar Közlöny*, 21 June. [Online]. Available at: https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html (Accessed: 21 June 2024).

Government of the Netherlands (2023) 'Security Strategy for the Kingdom of the Netherlands', 3 April. [Online]. Available at: https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands (Accessed: 21 June 2024).

Government Office of Sweden (2024) 'National Security Strategy' Stockholm, July 2024. [Online]. Available at: https://www.almendron.com/tribuna/wp-content/uploads/2021/01/national-security-strategy.pdf. (Accessed: 21 June 2024).

Governo Italiano (2021) 'Trattato tra la Repubblica Italiana e la Repubblica francese per una cooperazione bilaterale rafforzata' [Treaty between the Italian Republic and the French Republic for enhanced bilateral cooperation]. [Online]. Available at: https://www.governo.it/sites/governo.it/files/Trattato_del_Quirinale.pdf (Accessed: 21 June 2024).

Governo Italiano, Ministero della Difesa (2023) 'Documento Programmatico Pluriennale della Difesa per il triennio 2023-2025 [Defense multi-year planning document for the three-year period '[...] 2023-2025] Edizione 2023. [Online]. Available at: https://www.difesa.it/assets/allegati/2569/4acffd61-84fa-4df3-bdab-806066fa5d56.pdf (Accessed: 21 June 2024).

Grevi, G., Morillas, P., Soler i Lecha, E., Zeiss, M. (2020) 'Differentiated Cooperation in European Foreign Policy: The Challenge of Coherence', *EU IDEA Policy Paper*, No. 5. [Online]. Available at: https://www.epc.eu/content/PDF/2020/EU_IDEA-_challenge_of_coherence.pdf (Accessed: 21 June 2024).

Grevi, G. (2016) 'What Ambition for Defence in the EU?', *Italian Institute for International Political Studies*, 19 October 2016. [Online]. Available at: http://www.ispionline.it/it/pubblicazione/what-ambition-defence-eu-15855 (Accessed: 21 June 2024).

Grüll, P., Lawton, S. (2020) 'Sovereignty and solidarity: Germany's plans for the EU's foreign policy', *Euractive*, 29 June 2020. [Online]. Available at: https://www.euractiv.com/section/global-europe/news/sovereignty-and-solidarity-germanys-plans-for-the-eus-foreign-policy/ (Accessed: 21 June 2024).

Hill, C. (1990) 'European foreign policy: Power bloc, civilian model – or flop?' in Reinhardt, R. (ed.) *The Evolution of an International Actor*. Boulder, CO: Westview Press.

Honvédelmi Minisztérium (2020) 'A Közép-Európai Védelmi Együttműködés védelempolitikai igazgatói tanácskoztak' [Central European Defence Cooperation defence policy directors meet], 1 July. [Online]. Available at: https://honvedelem.hu/hirek/hazai-hirek/a-kozep-europai-vedelmi-egyuttmukodes-vedelempolitikai-igazgatoi-tanacskoztak.html (Accessed: 21 June 2024).

Howorth, J. (2017) 'EU–NATO Cooperation: The Key to Europe's Security Future', *European Security*, 26(3), pp. 454–459; https://doi.org/10.1080/09662839.2017.1352584.

Howorth, J. (2019) 'Differentiation in Security and Defence Policy', *Comparative European Politics*, 2019/17, pp. 261–277; https://doi.org/10.1057/s41295-019-00161-w.

Informal Meeting of Foreign Affairs Ministers (2016) 'Informal Meeting of Foreign Affairs Ministers', 2-3 September 2016. [Online]. Available at: http://www.eu2016.sk/en/political-and-expert-meetings/informal-meeting-of-foreign-affairs-ministers-gymnich (Accessed: 21 June 2024).

Ischinger, W. (2013) 'Germany's Foreign Policy Lacks Big Ideas', *The Guardian*, 29 November 2013. [Online]. Available at: https://www.theguardian.com/business/2013/nov/29/german-foreign-policy-coalition-caution (Accessed: 21 June 2024).

Jones, B. (2020) 'CSDP defence capabilities development', *Directorate-General for External Policies*, 10 January 2020. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/603482/EXPO_IDA(2020)603482_EN.pdf (Accessed: 21 June 2024).

Juncker, J-C. (2016) 'President Jean-Claude Juncker's State of the Union Address 2016', Brussels, 14 September 2016. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_110 (Accessed: 21 June 2024).

Juncker, J-C. (2017) 'President Jean-Claude Juncker's State of the Union Address 2017', Brussels, 13 September 2017. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165 (Accessed: 21 June 2024).

Juncker, J-C. (2018) 'State of the Union 2018 The Hour of European Sovereignty', Strasbourg, 12 September 2018. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_5808 (Accessed: 21 June 2024).

Kingdom of Belgium (2022) 'Stratégie de sécurité nationale' [National Security Strategy]. [Online]. Available at: https://www.egmontinstitute.be/app/uploads/2022/02/NVS_Numerique_FR.pdf (Accessed: 21 June 2024).

Kingdom of the Netherlands (2021) 'Spain-Netherlands Non-paper on Strategic Autonomy while Preserving an Open Economy', 25 March. [Online]. Available at: https://open.overheid.nl/documenten/ronl-fd3bbc94-f598-45b3-abbd-75bfd5b18b97/pdf (Accessed: 21 June 2024).

Kingdom of the Netherlands (2023) 'Joint Non-paper on Open Strategic Autonomy of the EU. Belgium, Finland, the Netherlands, Portugal, and Slovakia.', 19 July. [Online]. Available at: https://open.overheid.nl/documenten/5f3a6437-92b3-41bc-835a-e4d803ee6f6b/file (Accessed: 21 June 2024).

von der Leyen, U. (2021) 'State of the Union 2021', Strasbourg, 15 September 2021. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_4701 (Accessed: 21 June 2024).

Libek, E. (2019) 'European Strategic Autonomy: A Cacophony of Political Visions', *International Centre for Defence and Security*, 19 December 2019. [Online]. Available at: https://icds.ee/en/european-strategic-autonomy-a-cacophony-of-political-visions/ (Accessed: 21 June 2024).

Macron, E. (2017) 'Sorbonne Speech of Emmanuel Macron – Full text / English version', *Ouest-France*, 26 September 2017. [Online] Available at: https://international.blogs.ouest-france.fr/archive/2017/09/29/macron-sorbonne-verbatim-europe-18583.html (Accessed: 21 June 2024).

Manners, J. (2002) 'Normative Power Europe: A Contradiction in Terms?', *Journal of Common Market Studies,* 40(2), pp. 235–258; https://doi.org/10.1111/1468-5965.00353.

Manners, I. (2006) 'Normative power Europe reconsidered: beyond the cross-roads', *Journal of European Public Policy*, 13(2), pp. 182–199; https://doi.org/10.1080/13501760500451600.

Meijer, H., Wyss, M. (2018) *The Handbook of European Defence Policies and Armed Forces*. Oxford: Oxford University Press; https://doi.org/10.1093/oso/9780198790501.001.0001.

Meyer, Ch., Van Osch, T., Reykers, Y. (2022) 'The EU Rapid Deployment Capacity: This time, it's for real?', *European Parliament: Policy Department for External Relations, Directorate General for External Policies of the Union*, October 2022. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702568/EXPO_IDA(2022)702568_EN.pdf (Accessed: 21 June 2024).

Ministère de l'Europe et des Affaires Étrangères (2024) 'Meeting of the Weimar Triangle countries – Joint Statement by Foreign Ministers of France, Germany and Poland (12 February 2024)'. [Online]. Available at: https://www.diplomatie.gouv.fr/en/country-files/germany/the-weimar-triangle/article/meeting-of-the-weimar-triangle-countries-joint-statement-by-foreign-ministers (Accessed: 21 June 2024).

Ministry of Defence of the Czech Republic (2022) 'Armaments and Defence Industry. Development Support Strategy of the Czech Republic till 2030' Prague, May 2022. [Online]. Available at: https://www.army.cz/assets/en/ministry-of-defence/basic-documents/327_22_strategie_vyzbrojovani_en.pdf (Accessed: 21 June 2024).

Ministry of Foreign Affairs of Denmark (2023) 'Danish Foreign and Security Policy Strategy', May 2023. [Online]. Available at: https://um.dk/en/foreign-policy/foreign-and-security-policy-2023 (Accessed: 21 June 2024).

Ministry of Foreign Affairs of the Czech Republic (2023) 'Security Strategy of the Czech Republic' Prague, 1 September 2023. [Online]. Available at: https://mzv.gov.cz/jnp/en/foreign_relations/security_policy/security_strategy_of_the_czech_republic/index$2548.html?action=setMonth&year=2019&month=9 (Accessed: 21 June 2024).

Missiroli, A. (ed.) (2003) *From Copenhagen to Brussels. European defence: core documents*. Paris: EU Institute for Security Studies, Chaillot Papers, Vol. 4, No. 67, pp. 36–39. [Online]. Available at: www.iss.europa.eu/sites/default/files/EUISSFiles/cp067e.pdf (Accessed: 21 June 2024).

Molnár, A. (2018) *Az Európai Unió külkapcsolati rendszere és eszközei. A külkapcsolatoktól a kül-, a biztonság- és védelempolitikáig* [The European Union's external relations system and instruments. From external relations to foreign, security and defence policy]. Budapest: Dialóg Campus.

Molnár, A. (2022) 'The idea of a European Security and Defence Union' in Molnár, A., Fiott, D., Asderaki, F., Paile-Calvo, S. (eds.) *Challenges of the Common Security and Defence Policy: ESDC 2nd Summer University Book*. Luxembourg: Publications Office of the European Union, pp. 19–36; https://doi.org/10.2855/361636.

Molnár, A., Csiki Varga, T. (2023) 'EU Power (Strategic Autonomy) in a Multipolar World' in Molnár, A., Jakusné-Harnos, É., Szente-Varga, M. (eds.) *Security, Resilience and Sustainability of the European Union*. Budapest: Ludovika University Press, pp. 9–32. Available at: https://www.eusecure.org/_files/ugd/44ea33_509659f7b4b84e9aabc2d8f43109f821.pdf (Accessed: 21 June 2024).

Molnár, A. (2019b) 'PESCO' in Krajnz, Z. (ed.) *Hadtudományi lexicon* [Encyclopaedic lexicon]. Budapest: Dialóg Campus Kiadó, pp. 880–881.

Moravcsik, A. (2010) 'Europe: The Second Superpower', *Current History,* 109(725), pp. 91–98; https://doi.org/10.1525/curh.2010.109.725.91.

National Security Bureau of the Republic of Poland (2020) 'National Security Strategy of the Republic of Poland' Warsaw, 12 May 2020. [Online]. Available at: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf (Accessed: 21 June 2024).

de Neve, J. (2007) 'The European Onion? How differentiated integration is reshaping the EU', *Journal of European Integration*, 29(4), pp. 503–521; https://doi.org/10.1080/07036330701502498.

Nissen, Ch. (2021) 'European Strategic Autonomy as seen from Denmark: Essentially Contested' in Lewander, J. (ed.) *Strategic Autonomy – Views from the North. Perspectives on the EU in the World of the 21st Century*, Stockholm: Swedish Institute for European policy studies, Report no. 1op, December 2021. [Online]. Available at: https://www.sieps.se/globalassets/publikationer/2021/2021_1op.pdf (Accessed: 21 June 2024).

Nováky, N. (2017) 'The European Security and Defence Union: how should it look like?', *Vocal Europe*, 13 November 2017. [Online]. Available at: https://www.vocaleurope.eu/the-european-security-and-defence-union-how-should-it-look-like/ (Accessed: 21 June 2024).

Nye, J.S. (2023) *Soft Power and Great-Power Competition*. Singapore: Springer Singapore; https://doi.org/10.1007/978-981-99-0714-4.

von Ondarza, N. (2013) 'Strengthening the Core or Splitting Europe? Prospects and Pitfalls of a Strategy of Differentiated Integration', *SWP Research Papers*, No. 2 (March). [Online]. Available at: https://www.swp-berlin.org/en/publication/eu-differentiated-integration (Accessed: 21 June 2024).

Orłowski, T. (2023) 'European Strategic Autonomy Remains Conveniently Broadly Defined', *Visegard Insight*, 29 September 2023. [Online]. Available at: https://visegradinsight.eu/european-strategic-autonomy-remains-conveniently-broadly-defined/ (Accessed: 21 June 2024).

Partito Democratico (2018) 'Il nostro futuro si chiama Stati Uniti d'Europa' [Our future is called the United States] *Partito Democratico*, 15 February. [Online]. Available at: www.partitodemocratico.it/approfondimenti/unione-europea-stati-uniti-europa/ (Accessed: 21 June 2024).

Phelan, W. (2012) 'What Is Sui Generis About the European Union? Costly International Cooperation in a Self-Contained Regime.', *International Studies Review*, 14(3), pp. 367–385; https://doi.org/10.1111/j.1468-2486.2012.01136.x.

Presidencia del Gobierno (2021) 'Estrategia de Seguridad Nacional' [National Security Strategy]. [Online]. Available at: https://administracionelectronica.gob.es/pae_Home/en/pae_Actualidad/pae_Noticias/Anio2022/Enero/Noticia-2022-01-07-Estrategia-Nacional-Seguridad-2021.html?idioma=en (Accessed: 21 June 2024).

Puig-Soler, S. (2021) 'The European Peace Facility' in Rehrl, J. (ed.) *Handbook on CSDP, The Common Security and Defence Policy of the European Union*. 4th edn. Vienna: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, pp. 103–109. [Online]. Available at: https://www.egmontinstitute.be/app/uploads/2021/06/CSDP-HANDBOO-4th-edition.pdf (Accessed: 21 June 2024).

Recchia, S. (2020) 'A legitimate sphere of influence: Understanding France's turn to multilateralism in Africa', *Journal of Strategic Studies,* 43(4), pp. 508–533; https://doi.org/10.1080/01402390.2020.1733985.

Regulation (EU) 2023/1525 of the European Parliament and of the Council of 20 July 2023 on supporting ammunition production (ASAP) (2023) OJ L 186/7, Brussels, 24 July 2023. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1525&qid=1695904709752 (Accessed: 21 June 2024).

Regulation (EU) 2023/2418 of the European Parliament and of the Council of 18 October 2023 on establishing an instrument for the reinforcement of the European defence industry through common procurement (EDIRPA) (2023) OJ L, 26 October 2023. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302418 (Accessed: 21 June 2024).

Renzi, M. (2018) 'Europa', *matteorenzi.it*, 2018. [Online]. Available at: www.matteorenzi.it/europa/ (Accessed: 21 June 2024).

Republic of Croatia (2017) 'National Security Strategy'. [Online]. Available at: https://www.soa.hr/files/file/National-Security-Strategy-2017.pdf (Accessed: 21 June 2024).

Republic of Estonia, Ministry of Defence (2015) 'Baltic Defence Co-operation', 18 June 2015. [Online]. Available at: https://www.kaitseministeerium.ee/en/objectives-activities/international-cooperation/baltic-defence-co-operation (Accessed: 21 June 2024).

República Portuguesa (2013) 'Conceito Estratégico, de Difesa Nacional. Strategic Concept of National Defence.' *Defesa Nacional*, 2013. [Online]. Available at: https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Strategic-Concept-of-National-Defence.pdf (Accessed: 21 June 2024).

République Française (2022) 'National strategic review 2022' *Secrétariat général de la défense et de la sécurité nationale*, 9 November. [Online]. Available at: https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf (Accesssed: 21 June 2024).

Reykers, Y. (2017) 'EU Battlegroups: High costs, no benefits', *Contemporary Security Policy*, 38(3), pp. 457–470; https://doi.org/10.1080/13523260.2017.1348568.

Reykers, Y. (2019) 'A permanent headquarters under construction? The Military Planning and Conduct Capability as a proximate principal', *Journal of European Integration*, 41(6), pp. 783–799; https://doi.org/10.1080/07036337.2019.1599882.

Ringsmose, J., Rynning, S. (2017) 'The NATO Response Force: A qualified failure no more?', *Contemporary Security Policy,* 38(3), pp. 443–456; https://doi.org/10.1080/13523260.2017.1350020.

Romania Presidential Administration (2020) 'National Defence Strategy, 2020-2024: "Together for a safe and prosperous Romania in a world marked by new challenges"' Bucharest, 2020. [Online]. Available at: https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf (Accessed: 21 June 2024).

Saint-Malo declaration [Joint Declaration issued at British-French Summit] (1998) Saint-Malo, 4 December 1998. [Online]. Available at: https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf (Accessed: 21 June 2024).

Schnitzl, G. (2023) 'EDIRPA/EDIP: Risks and opportunities of future joint procurement incentives for the European defence market', *Armament Industry European Research Group, French Institute for International and Strategic Affairs*, March 2023. [Online]. Available at: https://www.iris-france.org/wp-content/uploads/2023/03/ARES-81-Policy-paper.pdf (Accessed: 21 June 2024).

Silva, P.M., Zachary, S. (2020) 'Economic interdependence and economic sanctions: a case study of European Union sanctions on Russia', *Cambridge Review of International Affairs,* 33(2), pp. 229–251; https://doi.org/10.1080/09557571.2019.1660857.

Slovak Republic (2021) 'Security Strategy of the Slovak Republic'. [Online]. Available at: https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf (Accessed: 21 June 2024).

Smith, K. (2005) 'Beyond the civilian power EU debate', *Politique européenne*, 2005/3, pp. 63–82; https://doi.org/10.3917/poeu.017.0063.

Spain's National Office of Foresight and Strategy Spain's National Office of Foresight and Strategy (2023) 'Resilient EU2023. A future-oriented approach to reinforce the EU's Open Strategic Autonomy and Global Leadership'. [Online]. Available at: https://futuros.gob.es/sites/default/files/2023-09/RESILIENTEU2030.pdf (Accessed: 21 June 2024).

Stavridis, S. (2001) '"Militarizing" the EU: the Concept of Civilian Power Europe Revisited', *The International Spectator*, 36(4), pp. 43–50; https://doi.org/10.1080/03932720108456945.

de Sutter, C. (2020) 'Europe's Road to strategic autonomy: Summarising the concrete steps taken', *Finabel*, 3 June 2020. [Online]. Available at: https://finabel.org/europes-road-to-strategic-autonomy-summarising-the-concrete-steps-taken/ (Accessed: 21 June 2024).

Swedish Ministry of Defence (2023) 'The Swedish Defence Commission's report on security policy' *The Defence Commission's Secretariat*, 19 June. [Online]. Available at: https://www.regeringen.se/contentassets/de808e940116476d8252160c58b78bb7/sammandrag-pa-engelska-av-allvarstid-ds-202319.pdf (Accessed: 21 June 2024).

Tocci, N. (2008) 'When and why does the EU act as a normative power in its neighbourhood?' in Heisbourg, F., Tocci, N., Hamilton, D., Makarychev, A.S., Xiang, L., Kumar, R. (eds.) *What Prospects for Normative Foreign Policy in a Multipolar World?*. CEPS ESF Working Papers, No. 29, pp. 1−6. [Online]. Available at: https://www.files.ethz.ch/isn/88204/29_Full.pdf (Accessed: 21 June 2024).

Törő, Cs. (2014) 'Accommodating Differences within the CSDP: Leeway in the Treaty Framework?' in Blockmans, S. (ed.) *Differentiated Integration in the EU. From the Inside Looking*. Brussels: Centre for European Policy Studies, pp. 57–74.

Torreblanca, J.-I., Jorge-Ricart, R. (2022) 'The US-EU Trade and Technology Council (TTC): State of Play, Issues and Challenges for the Transatlantic Relationship', *EsadeEcPol – Center for Foreign Policy*, *European Council on Foreign Relations*, Paper Series No. 1, January 22. [Online]. Available at: https://www.esade.edu/ecpol/wp-content/uploads/2022/12/AAFF_EcPol-OIGI_PaperSeries_ENG_def_jan22.pdf (Accessed: 21 June 2024).

Treaty establishing a Constitution for Europe (2004) OJ C 310/1, 16 December 2004. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ%3AC%3A2004%3A310%3ATOC (Accessed: 21 June 2024).

Treaty no. 5476. United Kingdom of Great Britain and Northern Ireland, Greece and Turkey and Cyprus (1960) Nicosia, 16 August 1960. [Online]. Available at: https://www.mfa.gr/images/docs/kypriako/treaty_of_establishment.pdf (Accessed: 21 June 2024).

Tsitsikostas, G. (2021) 'Challenges of Military Operations and Missions' in Rehrl, J. (ed.) *Handbook on CSDP, The Common Security and Defence Policy of the European Union*. 4th edn. Vienna: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, pp. 86–92. [Online]. Available at: https://www.egmontinstitute.be/app/uploads/2021/06/CSDP-HANDBOO-4th-edition.pdf (Accessed: 21 June 2024).

Varga, G. (2017) *Towards European Strategic Autonomy? Evaluating the New CSDP Initiatives*. Budapest: Institute for Foreign Affairs and Trade. [Online]. Available at: https://www.academia.edu/34771843/Towards_European_Strategic_Autonomy_Evaluating_the_New_CSDP_Initiatives (Accessed: 21 June 2024).

de Vasconcelos, Á. (2009) 'Introduction – 2020: defence beyond the transatlantic paradigm' in de Vasconcelos, A. (ed.) *What ambitions for European defence in 2020?*. Paris: EU Institute for Security Studies, pp. 15–26. [Online]. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/What_ambitions_for_European_defence_in_2020_0.pdf (Accessed: 21 June 2024).

Visegrad Group (2014) 'Visegrad Group Defence Cooperation'. [Online]. Available at: http://www.visegradgroup.eu/about/cooperation/defence (Accessed: 21 June 2024).

von Weitershausen, I., Schafer, D., Wessels, W. (2020) 'A 'Primus Inter Pares' in EU Foreign Policy? – German Leadership in the European Council during the Libyan and Ukrainian Crises', *German Politics,* 29(1), pp. 42–58; https://doi.org/10.1080/09644008.2019.1583328.

Wagner, W. (2017) 'Liberal Power Europe', *Journal of Common Market Studies,* 55(6), pp. 1398–1414; https://doi.org/10.1111/jcms.12572.

Wallace, W. (1999) 'The Sharing of Sovereignty: The European Paradox', *Political Studies,* 47(3), pp. 503–521; https://doi.org/10.1111/1467-9248.00214.

Zandee, D., Deen, B., Kruijver, K., Stoetman, A. (2020) 'European strategic autonomy in security and defence. Now the going gets tough, it's time to get going.', *Clingendael Report*, December 2020. [Online]. Available at: https://www.clingendael.org/sites/default/files/2020-12/Report_European_Strategic_Autonomy_December_2020.pdf (Accessed: 21 June 2024).

Zandee, D., Stoetman, A. (2022) 'Realising the EU Rapid Deployment Capacity: opportunities and pitfalls', *Clingendael*, Policy Brief, October 2022. [Online]. Available at: https://www.clingendael.org/sites/default/files/2022-10/Policy_brief_Rapid_Deployment_Capacity.pdf (Accessed: 21 June 2024).

EU-Kommissionspräsident Juncker für europäische Armee (2015) *Welt*, 8 March 2015. [Online]. Available at: https://www.welt.de/newsticker/news1/article138177624/EU-Kommissionspraesident-Juncker-fuer-europaeische-Armee.html (Accessed: 21 June 2024).

Im Wortlaut, Pressekonferenz von Bundeskanzlerin Angela Merkel und Präsident Emmanuel Macron beim 19. Deutsch-Französischen Ministerrat [Text of the press conference by Federal Chancellor Angela Merkel and President Emmanuel Macron at the 19th Franco-German Council of Ministers] (2017) *Bundesgreigung*, 13 July 2017. [Online]. Available at: https://www.bundesregierung.de/Content/DE/Mitschrift/Pressekonferenzen/2017/07/2017-07-13-pk-merkel-marcon-paris.html (Accessed: 21 June 2024).

NATO is not enough, EU needs an army (2016) *EurActiv*, 9 March 2016. [Online]. Available at: https://www.euractiv.com/section/global-europe/news/juncker-nato-is-not-enough-eu-needs-an-army/ (Accessed: 21 June 2024).

Chapter 2

Reinforcing European Defence Industry for Times of Great Power Conflicts

Tamás Csiki Varga

Abstract

With the European security environment deteriorating and destabilising in the 2010s, European defence – particularly the European defence industry – has gained heightened attention since 2022, as evidenced by Russia's renewed aggression towards Ukraine. European countries have since attempted to efficiently address the dilemma of short-term production and stock replenishment versus long-term research, development, and innovation to offset the unpreparedness of European armed forces to fight protracted high-intensity wars. Accordingly, this chapter aims to outline the demand–supply equation of the European defence industry leading up to the Hungarian EU Presidency in 2024, and the adoption of the first-ever European Defence Industrial Strategy. This strategy aims to identify the drivers for developing the European Defence Industrial and Technological Base (EDTIB) as a defence ecosystem by the 2030s, enabling the sustainable provision of arms that European countries may need to defend themselves on European soil and uphold their interests.

The following analysis provides an overview of the trends leading up to 2024 for enhancing European defence industrial production, research and development. The chapter is structured as follows: first, it outlines the dynamics of the changing European security environment and threat perception, followed by an assessment of European capability gaps and policy responses aimed at closing these gaps, including an improved record of defence investments.

The main argument is that despite the constraints of EDTIB in the early 2020s, such as the effects of three decades of underinvestment, fragmentation of production capacities, shortcomings in providing raw materials and access to cutting-edge technology,

Tamás Csiki Varga (2024) 'Reinforcing European Defence Industry for Times of Great Power Conflicts'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 73–108. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_2

as well as shortages of manufacturing capabilities and skilled manpower, there are nevertheless opportunities to remedy this situation. Drivers for comprehensive and efficient European defence industrial cooperation are being developed, including better-aligned strategic planning and defence capability development, currently underpinned by increasing defence spending, extensive joint defence procurements, and research and development (through the European Defence Industry Reinforcement through Common Procurement Act and the European Defence Industry Programme, supported by Permanent Structured Cooperation, the European Defence Fund, and the European Peace Facility).

Keywords: defence industry, strategy, armament, procurement, European Defence Technological and Industrial Base

1. An ambivalent strategic landscape determining armed forces development and defence industry trends in Europe

Strategic trends determining the current security environment and wider framework of European defence efforts can be traced back to the post-Cold War transformation of European defence architecture. This not only relates to institutions (North Atlantic Treaty Organization (NATO) and EU enlargement, institutionalised EU defence policy ambitions), but also armed forces' development (and downsizing), resource (re-)allocation and defence industry transformation. The approximately 25 years between the end of the Cold War and Russia's illegal annexation of Crimea in 2014 triggered a fundamental weakening in most aspects, followed by a slow reversal of the negative trends in post-Crimea shock. Defence efforts further accelerated since the 2022 escalation of the Russo-Ukrainian War, bringing back old, unresolved puzzles and raising new questions for European defence. In this 35-year period, the strategic milestones were 2008–2009, 2014–2015 and 2022, as briefly assessed below, which fundamentally determined the troubled state of the European Defence Industrial and Technological Base (EDTIB) as we know it in 2024.

1.1. The "peace dividend" of the 1990s

After the Cold War ended, amid the diminishing risk of a major military confrontation with Russia, countries in Western Europe downsized their armed forces, as exemplified by the International Institute for Strategic Studies (IISS). In 1990, West Germany fielded 215 combat battalions, Italy 135, France 106 and the United Kingdom 94, supported by the U.S. European Command's (EUCOM) 99 battalions. Meanwhile by 2015, Germany could field only 34, Italy 44, France 43 and the United

Kingdom 50, together with U.S. EUCOM's 14 battalions.[1] According to the Stockholm International Peace Research Institute (SIPRI), between 1989 and 1998 (the lowest point), NATO Member States' cumulative defence budgets decreased by 26% in real terms, after which it only reached 1989 levels by 2004.[2] Downsizing trends did not differ in Central Europe, driven by political transformation and economic scarcity.

This "peace dividend", namely the unused resources from defence converted for civilian purposes, was welcomed by European countries, but it also inevitably led to chronic underfinancing in the armed forces, and the downsizing of Europe's defence industrial capacities. During the Cold War, European governments were willing to sustain larger armed forces and finance a degree of defence industrial overcapacity to ensure reliable access to equipment at scale; when the Cold War ended, the emphasis changed from readiness to efficiency.[3] Consequently, Europe's defence industrial capacities have been likened to artisan facilities, crafting a few sophisticated products,[4] losing readiness for high-intensity, large-scale production. During these years, arms exports largely contributed to the survival of national arms industries that were gradually losing government funding, domestic orders and manpower; thus unwillingly restructuring to fit into the new defence environment.

1.2. Effects of the 2008 global economic crisis: the dual spiral of diminishing capabilities

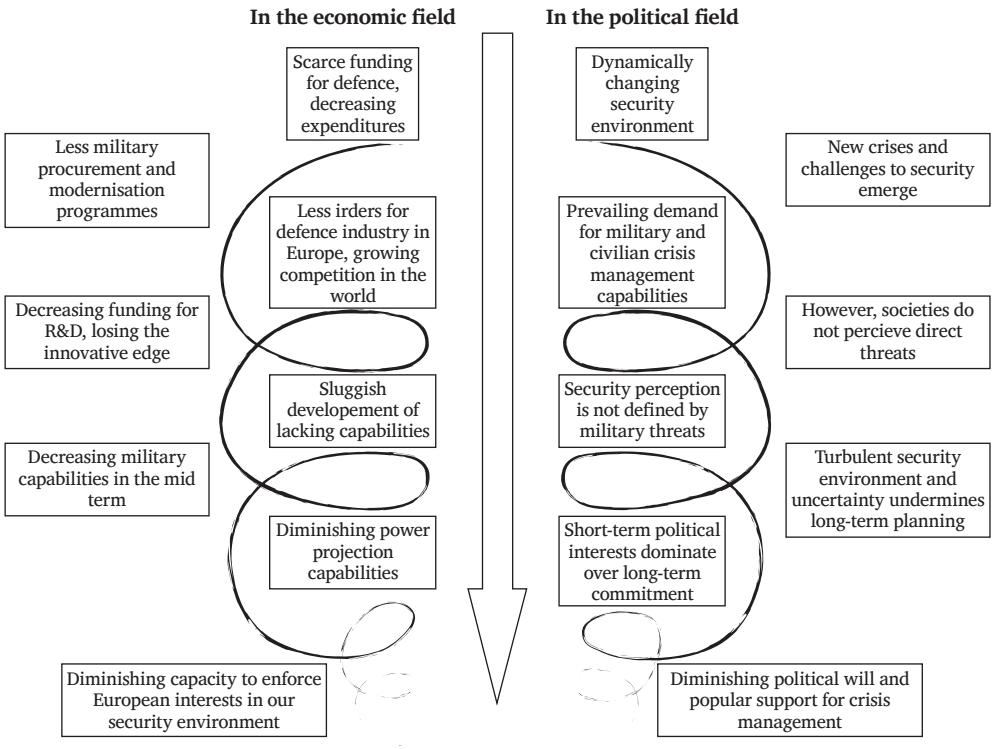
Following mild "normalisation" after the turn of the millennium, the 2008–2009 economic crisis brought about a strategic turning point. First, normalisation was driven by the changing military operational profile of European armed forces engaging in international interventions in Afghanistan, Iraq and Libya, along with the United States, followed by long-term multinational stabilisation operations. Despite providing a spending boost (2004–2010: +22%[5]) for militaries and some procurement of equipment necessary for overseas missions, these developments did not alter the overarching trend of shrinking force structures and diminishing stockpiles, while ageing military equipment was gradually replaced in most armed forces, often through off-the-shelf procurement. Off-the-shelf procurement often occurred outside Europe, particularly in the United States, undermining the consolidation of the European defence industry.

The 2008 global economic crisis had a severe impact on European countries; overall defence spending decreased by 10.1% in NATO and by 9.5% in NATO Europe between 2008 and 2014.[6] Summing up the strategic developments from 2008–2014 – also the period between the Russia–Georgia war and Russia's hybrid war on Ukraine

1 Barrie et al., 2020, p. 2.
2 SIPRI, 2023. Defence data are registered in constant USD 2022.
3 Aries, Giegerich and Lawrenson, 2023, p. 8.
4 Karsenti, 2023.
5 SIPRI, 2023. Defence data are registered in constant USD 2022.
6 SIPRI, 2023. Defence data are registered in constant USD 2022.

– one can observe two parallel processes in political and economic domains, bringing about the degradation of military capabilities and the weakening of military tools of European power. As Csiki argued in 2014, these processes can be modelled as a 'dual spiral of diminishing capabilities' (Figure 1).[7]

Figure 1: Dual spiral of diminishing capabilities[8]



In the economic domain, the process of capability loss was triggered by scarce resources as an outcome of the financial crisis, which evolved from a primary (debt) crisis into a secondary (fiscal–monetary) crisis, inducing significant societal and political consequences in several European countries, especially in Southern and Central Europe. Diminishing resources dedicated to the defence sector resulted in investment cuts in armament modernisation, research and development (R&D) as well as procurements for national armed forces in the short term. The reduced domestic orders and contract cuts for weapons systems and defence equipment increasingly forced European manufacturers to turn to

7 Csiki, 2014, pp. 49–50.
8 Csiki, 2014, p. 49.

the global market, where they faced increased competition from arms manufacturers from the United States and emerging powers, while their resources for cutting-edge R&D decreased. Consequently, missing military crisis management capabilities, such as strategic enablers, either had not (fully) been developed or suffered delays and shortcomings owing to lack of technological background and/or financing. This was especially apparent in multinational capability development programmes, where diverging national priorities in financial crisis management could seriously undermine joint programmes. The resulting medium-term loss of military capabilities also limited crisis management options, thereby reducing Europe's power projection ability and assertion of foreign policy interests in European neighbourhoods.[9]

In the political domain, the loss of capabilities stemmed from the interactions between external and internal factors. Externally, the rapid and dynamic deterioration of the security environment (emerging crises and new types of threats, such as regional instability triggered by the Arab Spring, civil war and strengthening terrorism) resulted in a sustained demand for military and civilian crisis management. However, European societies did not perceive direct, imminent military threats before 2014, because of economic hardships (rising living costs, high unemployment rates and decreasing social benefits). This lack of perceived threats at a time of resource scarcity obviously meant that it was difficult to advocate funding for defence at a sustainable level (not to mention increasing it) when the economic crisis turned people's attention towards non-military dimensions of security. In this environment, short-term interests, such as the effective management of the economic crisis and scarcity of resources, dominated long-term strategic planning necessary for meaningful capability development and long-term commitment required for yielding crisis management efforts. Overall, it highlighted the diminishing political will and popular support for sacrificing funds for the development of defence capabilities and refraining from a more active foreign policy and involvement in crisis management efforts in the European neighbourhood.

This situation was exemplified by Libya's intervention, initially initiated by European powers, and led mainly by France and the United Kingdom. The conduct of operations was sobering as European powers had to rely on the support of the United States within the NATO framework (dubbed as "leading from behind") regarding key operational enablers: intelligence, surveillance and reconnaissance (ISR), command and control (C2), aerial refuelling, electronic warfare as well as munitions. Although the United States was meant to merely provide unique capabilities, their forces flew over 50% of sorties and provided 80% of ISR and refuelling, 25% of airborne C2 and suppression of almost all enemy air defences (SEAD) capabilities.[10] With shortcomings remaining unresolved, a similar dynamic was

9 Mölling and Brune, 2011.
10 Wall and Christianson, 2023.

observed a decade later when allied countries hurriedly evacuated tens of thousands of people from Afghanistan in 2021. European countries lacked the necessary resources for air transport, air refuelling, ISR and even ground forces to effectively secure Kabul Airport.[11]

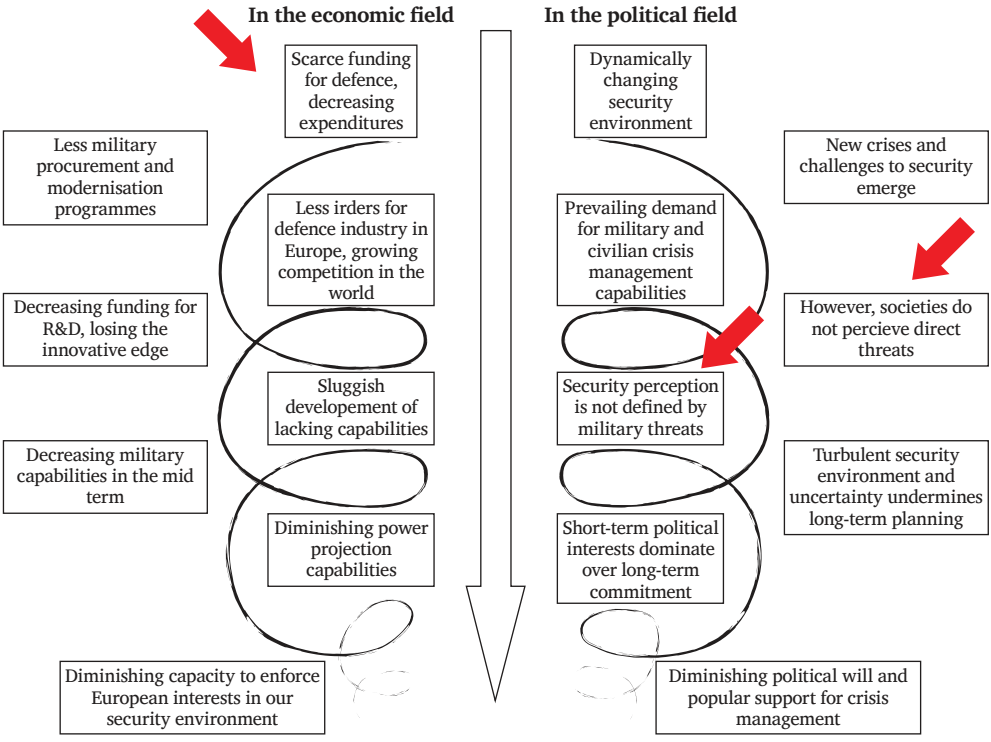
The key drivers of capability loss were as follows. While the incentives for strengthening European defence were clearly present, short-term economic necessities and interests, coupled with non-military threat perception, overruled the steps of medium- and long-term planning and capability development. Therefore, the two parallel downward spirals triggered the loss of military capabilities, further limiting political and popular support to actively shape the European security environment.

1.3. Breaking the dual spiral of diminishing capabilities after 2014

In the political field, the dual spiral of diminishing capabilities could be broken through changing European threat perceptions by identifying direct, imminent or close threats in the military domain. The increasingly new military challenges and threats that appeared in the deteriorating security environment – Russia's aggression against Ukraine, emergence of the "Islamic State" further destabilising Iraq and Syria, the influx of refugees into Europe, and subsequent acts of Islamist terrorism in Europe – increased the sense of threat in European societies. In most countries in Central and Eastern Europe, this also ignited a clearly visible sense of military threat.[12] This was reinforced by the intensification of political, media and societal discourses on defence matters. Meanwhile, in the economic field, recovery from recession first created the possibility of stopping the reduction of resources devoted to defence, and then gradually increasing military expenses. Figure 2 highlights this, as indicated by the arrows pointing to the steps in which the spirals had been broken.

11 Bergmann and Svendsen, 2023, p. 23.
12 Čižik, 2020; Kříž, 2020; Palczewska, 2020; Sarcinschi, 2020.

Figure 2: Breaking the dual spiral of diminishing capabilities[13]



The two institutions that played decisive roles in European security, the EU and NATO, also reacted to these changes. In December 2013, the European Council, arguing that defence matters in Europe,[14] restored defence policy issues on its agenda after a 5-year hiatus,[15] culminating in the adoption of the EU Global Strategy in 2016 and a package of proposals aimed at revitalising Common Security and Defence Policy (CSDP).[16] In parallel, NATO Member States decided to strengthen the alliance's deterrent, reactive and collective defence capabilities by adopting the

13 The figure was edited by the author.
14 Council of the European Union, 2013, p. 1.
15 Csiki, 2014, p. 1.
16 The EU began to establish frameworks and mechanisms for joint capability development and for filling capability gaps. The joint decision to establish Permanent Structured Cooperation (PESCO), with a special focus on the Crisis Response Operation Core (EUFOR CROC), the first project to initiate the coordination of Member States' defence planning processes based on the results of the Coordinated Annual Defence Review (CARD) and Capability Development Plan (CDP), supported by the Military Planning and Conduct Capability (MPCC), and resources dedicated to defence R&D by the European Commission (European Defence Fund, EDF) have all pointed to this direction.

Readiness Action Plan (RAP) at their 2014 Newport summit as well as increasing the defence spending of Member States to 2% of gross domestic product (GDP) ("defence pledge"),[17] followed by an "implementation" summit for executing RAP in Warsaw (2016). Consequently, NATO Europe's cumulative defence spending increased by 29.3% in real terms between 2014 and 2022.[18] In 2014, only three NATO allies fulfilled the 2% commitment (the United States, United Kingdom and Greece), and in 2022, ten countries achieved this benchmark, with the median average increasing to 1.65% of GDP for the 30-member alliance.[19] These political and economic developments demonstrate that the dual spiral of diminishing capabilities ended after 2014–2015. However, subsequent years did not fundamentally change the dynamics of European defence.

1.4. Effects of Russia's escalating aggression towards Ukraine (2022–present) on European defence efforts

The most recent strategic turning point in European defence was Russia's renewed and escalated aggression towards Ukraine in 2022, triggering a mostly unified and coordinated political, economic, humanitarian and military response from EU and NATO countries. Despite the United States whistleblowing since late autumn 2021, the large-scale Russian aggression, which started from 24 February 2022, was met with surprise and perceived as a strategic shock by most European countries, including the Great Powers, Germany and France.

In response, measures to strengthen European defence and deterrence both within EU and NATO frameworks were undertaken, in addition to a major effort to support Ukraine's self-defence. Strengthening European defence cooperation was built on five pillars: increasing defence investment, purchasing equipment to remedy capability shortcomings, resupplying equipment and armament stocks, increasing multinational cooperation and supporting the European defence industry, where possible. The toolbox for achieving these goals had also been widened: beyond the existing Permanent Structured Cooperation (PESCO) and European Defence Fund (EDF) frameworks, new initiatives – European Defence Industry Reinforcement through Common Procurement Act (EDIRPA) for short-to-mid-term and European Defence Industry Programme (EDIP) for mid-to-long-term defence investment and procurement – were created (more details later in this chapter), and new ways of joint financing, for example through European Peace Facility (EPF), were considered.[20]

Complementing the EU response, NATO also took decisive steps framed within the Madrid Summit declaration, also identifying the Russian Federation as 'the most

17 Csiki, Tálas and Varga, 2014, pp. 112–128.

18 SIPRI, 2023. Defence data are registered in constant USD 2022.

19 NATO, 2022, pp. 2–3.

20 PESCO: Permanent Structured Cooperation; EDF: European Defence Fund; EDIRPA: European Defence Industry Reinforcement through Common Procurement Act, EDIP: European Defence Investment Programme.

significant and direct threat to allies' security and to peace and stability in the Euro–Atlantic area'.[21] These steps included strengthened forward defence across eastern flank Member States through more forward-deployed combat formations, higher levels of readiness, prepositioning equipment, reinforced allied deterrence posture and readiness through enhanced NATO Response Force, dubbed the new NATO Force Model.

2. European military balance of the early 2020s – military and defence industrial capabilities

The 2022 escalation of the Russo-Ukrainian War ended "Europe's geopolitical holiday";[22] the 25 years of peace in Europe, which in historical perspective was rather an anomaly – an exception – not the norm. This break from the comfortable practice of outsourcing European defence – particularly deterrence – to the United States should cease in the 2020s. However, at present, European military and defence industrial capabilities are weak and fragmented, owing to decades of underinvestment. Faced with degrading capabilities driven by the effects of the 2008–2009 economic crisis summarised above, experts have warned that European countries may shift to maintaining "bonsai armies"[23] as in the 2010s. A decade later, the assessment continues to be dire, indicating that as an outcome of these trends, 'the armed forces in European NATO and European Union member states are hollowed out, plagued by unserviceable equipment and severely depleted ammunition stocks.'[24]

2.1. Capability gaps in the early 2020s

We can obtain a glimpse of changing European military capabilities – the quantity of assets in European countries' armed forces – by exploring the IISS Military Balance+ database, which offers a quantitative overview and qualitative assessment in this regard. These data show a sizeable decrease in European military assets available across many major arms categories between 2014 and 2023, along with a higher degree of heterogeneity in the platforms operated (Table 1). In comparison, the U.S. Armed Forces operates a single type of main battle tank (versus 11 in Europe), six types of armoured fighting vehicles (versus 49 in Europe) and six types of fighters (versus 19 in Europe).[25]

21 NATO, 2023.
22 Commijs, 2019.
23 Anderson et al., 2016, pp. 13–16.
24 Aries, Giegerich and Lawrenson, 2023, p. 7.
25 Bergmann and Besch, 2023.

Table 1: The changing equipment inventories of EU Member States in major arms, 2014–2023[26]

Major arms type	**"Active" inventories of EU-27 in 2014** *(No. of assets/ systems)*	**"Active" inventories of EU-27 in 2023** *(No. of assets/ systems)*	**Change** *(%)*	**Number of design families operated**
Main battle tank	4,657	3,885	–17%	11
Armoured fighting vehicle (APCs, IFVs)	21,259	20,344	–4%	49
Artillery (towed, self-propelled, MLRS)	4,723	4,789	+1%	35
Fighter (fighter, fighter-ground-attack)	1,721	1,513	–12%	19
Transport plane (light, medium, heavy)	561	543	–3%	25
Tanker aircraft	54	25	–54%	5
Attack helicopter	257	278	+8%	5
Air defence system (SAM launcher)	1,085	1,043	–4%	26

Aligning with the legacy of operational capability gaps in the 2010s mentioned earlier, the list of strategic enablers was either still missing or available only to the largest allies or the United States by the 2020s. Therefore, it would be extremely difficult to replace or substitute for European countries in the short-to-mid-term. Critical dependencies included strategic reconnaissance, surveillance, intelligence and target acquisition capabilities; command, control and communications systems, including space assets; deployable operational commands above the division level; deployable air force commands; theatre air defence; and missile defence, including early warning systems, long-range bomber forces and significant numbers of fifth-generation fighter aircraft. European States also have limited capabilities in long-range precision strikes, including surface-to-surface cruise missiles, aerial refuelling, strategic and tactical airlifts, and special operations aircraft. A conflict with

26 IISS, 2023. All data on European armed forces are derived from the Military Balance+ database, compiled and assessed by the author. The set includes all current EU Member States for both 2014 and 2023 (excluding the United Kingdom and European NATO members). The table was compiled by the author.

a major regional power would have seriously tested the capabilities of European naval forces, and the ability to disembark from the entry force (an EU battlegroup, for example) in a crisis management operation would also be questioned. Based on simulations and modelling, it was estimated that EU Member States would have the necessary capabilities to conduct short-term rescue and evacuation operations and humanitarian operations on their own, provided they mobilise the assets at their disposal. However, after Brexit, the naval capabilities of EU-27 fell short in humanitarian operations; and if these were parallel or long-term requirements, they would already exceed European operational capabilities.[27]

European enabling capabilities have been severely limited, particularly in the air domain. According to Bergmann and Svendsen, European countries operate approximately 35 relevant airborne C2 platforms (compared to 120 U.S. aircraft), approximately 150 air-to-air refuelling aircraft (compared to almost 450), a few dozen relevant aerial ISR aircraft (compared to 150) and about 200 unmanned aircraft (compared to over 900). Europe is completely reliant on the United States regarding electronic warfare and SEAD capabilities. Regarding short-to-medium-range air defence, European countries' stocks have been severely depleted by military aid provided to Ukraine, particularly regarding Soviet legacy systems operated by eastern flank NATO members. For long-range air and missile defence, European countries have very limited capabilities, relying on a few surface-to-air systems (Patriot, SAMP/T), and lack meaningful capabilities in the service of advanced threats and long-range weapons, such as high-velocity missiles and hypersonic glide vehicles. Regarding the navy, European countries retired one-third of their main surface combatant ships.[28]

The European Defence Agency's (EDA) Coordinated Annual Review on Defence (CARD) report, first published in November 2020, identified 55 specific capability development areas where EU Member States could/should make meaningful progress. These included 17 land, 14 air, 12 naval, 5 joint force and strategic, 4 space and 3 cyber theatre capabilities. In addition, 56 defence R&D opportunities were identified, as well as operational cooperation opportunities in the areas of force projection, non-kinetic engagement, force protection and capability development. The 55 areas were grouped into 6 clusters to provide guidance for the coordination of national capability development and defence R&D plans. For example, in the PESCO framework and with the support of EDF. The six key cluster areas identified were general-purpose tank type, individual military equipment, surface patrol vessel type, anti-drone weapon systems and anti-access, area denial devices, space capabilities and military mobility. These areas need to be supported by defence industry R&D in artificial intelligence (AI), cyber defence, new sensor technologies, materials, energy-efficient propulsion systems, unmanned devices and robotics.[29] In its assessment

27 Sabatino et al., 2020.
28 Bergmann and Svendsen, 2023, pp. 23–24.
29 European Defence Agency, 2020.

of the 2022 CARD review, the EDA identified essentially the same areas for development in terms of defence resource gaps and capability requirements based on the first lessons learnt from the Russo-Ukrainian War, underlining the need for the European defence industry to play a leading role in both manufacturing and R&D.[30]

Even in early 2024, the EU's strategic capability to act was limited to low-intensity operations in terms of available military capabilities. To provide higher-intensity operational capabilities, we have two options: either continue to rely on NATO, including the U.S. military capabilities to a decisive extent, or dynamically develop EU capabilities in the areas outlined above, and devise European national capabilities, with Member States making more of them available to the EU.

2.2. European policy responses to address shortcomings in defence

Policy action building on the adoption of the EU Global Strategy (2016) was supported by various initiatives, such as the Implementation Plan on Security and Defence, European Defence Action Plan: Towards a European Defence Fund, initiation of PESCO and EDF, and creation of the Directorate-General post for Defence Industry and Space (DG DEFIS). However, as Csernatoni pointed out, EU Member States did not share a common assessment of geopolitical threats and challenges;[31] thus a two-year joint assessment process was carried out to formulate 'an ambitious and actionable Strategic Compass, making the best use of the entire EU toolbox'.[32] In 2022, the Strategic Compass provided the operationalisation of the Global Strategy – thus actually serving as a security and defence strategy – used (among others) to define the capability requirements of the EU's military operational vision for the new Headline Goal, covering the next 10-year period.[33]

In this process, EDTIB was financed through the EU's Framework Programmes for Research and Innovation (2014–2020) and Horizon Europe (2021–2027), realised within the Pilot Projects (2015–2018), Preparatory Action on Defence Research (2017–2019), European Defence Industrial Development Programme (2019–2020) and EDF (2021–2027) frameworks. Practically, the expansion of the EU toolbox has gradually augmented resources available in this area (see details below). Not only the EDF (around 7 billion euros) has been mobilised, but additional research and industrial policy resources as well: the Digital Europe Programme (around 6.7 billion euros), the Horizon Europe (around 76 billion euros),[34] Space programme (around 13 billion euros) and Military Mobility Action Plan (1.69 billion euros).[35] Therefore, it can be assumed that this increase in resources will, in the long term, serve as an

30 European Defence Agency, 2022.
31 Csernatoni, 2021, p. 16.
32 Council of the European Union, 2021.
33 European External Action Service, 2022.
34 Zubascu, 2024.
35 Nádudvari, 2020, p. 8.

incentive for Member States to increase their participation in European capability development projects.[36]

As Fiott summarised, the EU's reactions to the strategic shock of Russia's renewed aggression towards Ukraine can be broadly classified into three main types: i) strategic reorientation (visible in the finalised provisions of the Strategic Compass), ii) defensive weaponisation (visible in the arms deliveries of the EU to Ukraine utilising EPF) and iii) industrial rehabilitation (an attempt to overhaul European defence industrial performance).[37]

Aligning with NATO's new Strategic Concept (Madrid, 2022), the Strategic Compass identified Russia as a challenger to the European status quo and security architecture and called for specific action through 80 policy recommendations to boost the robustness and speed of EU military action, build up resilience to internal and external shocks, develop military capabilities and strengthen partnerships.[38]

In terms of defensive weaponisation, the EPF, the off-budget tool of CSDP, was given the new role of providing lethal and non-lethal military support to Ukraine. Through three rounds of increases in 2022–2023, the EPF has a budget of over 12 billion euros, of which 5.6 billion euros have been mobilised to support Ukraine.[39] Moreover, 1.5 billion euros diverted for defence research from Horizon Europe on 1 February 2024 (mentioned above) have also been added to EDF through the Strategic Technologies for Europe Platform (STEP).[40]

As a direct reaction to the Russo-Ukrainian War, EU heads of state and government endorsed the European Commission's (EC) defence package of 15 February,[41] and on 11 March 2022, committed to 'bolstering European defence capabilities'.[42] The EC and EDA prepared the defence investment gap analysis in May 2022, underlining that EU Member States need to extend collaborative projects in production and procurement to create economies of scale, also identifying urgent investment gaps in producing ammunitions, and air and missile defence systems, as well as calling for phasing out legacy Soviet equipment and replacing them with European-made assets (such as main battle tanks, armoured fighting vehicles and artillery in the land domain).[43] The Act in Support of Ammunition Production (ASAP) served specifically to bolster 155 mm-calibre artillery rounds production. Next, EDIRPA was adopted in July 2022 with a budget of 500 million euros (later reduced to 300 million euros) as a short-term measure to boost the competitiveness and

36 European Defence Agency, 2022, p. 2.
37 Fiott, 2023, p. 449.
38 Council of the European Union, 2022a, pp. 2–5.
39 Council of the European Union, 2024.
40 Amid pressing priorities, Horizon Europe will have its 95.5-billion-euro budget cut by 1.2 billion in 2024, with 1.5 billion euros diverted to defence research, following the EU heads of state meeting of February 1, 2024. This signals both scarcity of resources and strong dedication to support defence R&D.
41 European Commission, 2022a.
42 Council of the European Union, 2022b, pp. 3–5.
43 European Commission, 2022b, p. 7.

efficiency of EDTIB in 2022–2024. EDIRPA will be followed by the creation of EDIP to further strengthen the EU's defence industry and production capabilities in the long-term, thus addressing the identified capability gaps.[44] The European Investment Bank was also assigned the role of financing dual-use research, development and innovation, civilian security infrastructure and cutting-edge technology projects.[45] By further strengthening institutional partnerships with the DG DEFIS, the EU Agency for the Space Programme, EDA and NATO, the new European Investment Bank (EIB) Strategic European Security Initiative will make financing up to eight billion euros available by 2027.[46]

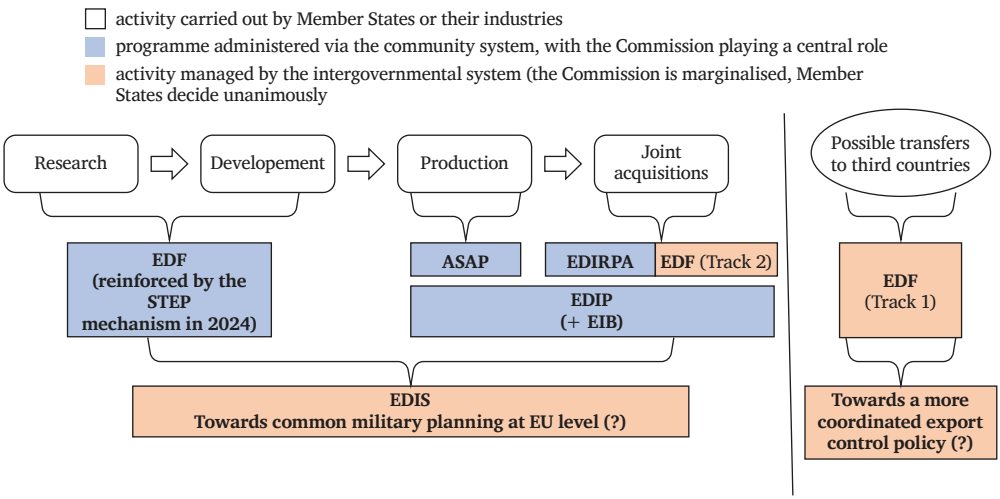
These steps outline a series of coherent actions aimed at creating policy and regulatory frameworks, as well as financial incentives for enhancing European defence industrial collaboration and increasing production capacities and capabilities in this field (Figure 3). EDF, reinforced by STEP, incentivises defence R&D, moving forward viable and marketable projects to production – exemplified by the tailored-to-needs support of ASAP in ammunition production – opening the possibility of joint acquisitions. The realisation of joint acquisitions can be underpinned by EDIRPA in the short term, occasionally supported by EPF, as again exemplified by the joint procurement of ammunition to replenish European stocks. Future production and acquisitions should be framed by EDIP, which also relies on the extra funding incentives of EIB. This process, encompassing defence R&D, production and joint acquisition, will soon be regulated by the upcoming European Defence Industrial Strategy (EDIS).[47] EDIS will rest on the strategic vision of the EU enshrined in the Global Strategy, translated into defence strategy and capability requirements through the Strategic Compass, potentially moving joint action towards common military planning at the EU level. As the case of direct military aid provided for Ukraine has shown, the possible transfer to third countries is also a viable option that policymakers should assess and regulate arms sales and the transfer of defence technology in general. Currently, this relates to the application of EPF for providing lethal and non-lethal military support, security assistance, etc. to third countries; however, for future applications, these considerations should be included in the EU-level unified arms export control policy (if adopted).

Figure 3 also illustrates that defence industrial activities are regulated and realised through three simultaneous strands of action: Member States and their (national or multinational) defence companies realise R&D, production and sale of procurement parties to acquisitions in the defence market; framework programmes and financial incentives (EDF, ASAP, EDIRPA, EDIP) are regulated and operated via the community system, with the EC playing a central role; while EPF and the

44 Andersson and Cramer, 2023, p. 42.
45 European Investment Bank, 2022.
46 European Investment Bank, 2023.
47 For a preliminary assessment of the key topics of EDIS and the hurdles related to its adoption, anticipated for early 2024, see: Fiott, 2024.

negotiated adoption of further strategic framework documents (such as EDIS or an EU arms export control policy) should be managed through intergovernmental co-operation and decisions, where the EC is marginalised and Member States decide unanimously.

Figure 3: Current frameworks and regulations for supporting EDTIB through collaborative action and underlying programmes.[48]



It is worth emphasising that the incentives agreed upon since February 2022 are formulated based on a different planning assumption during the 2000s and the 2010s, the starting points for preparing for crisis management in the European neighbourhood, as well as providing the necessary capabilities for such operations. Starting from 2022, preparing for deterrence and defence against a near-peer or peer-to-peer adversary, namely Russia, became the new focus of capability planning, bringing many apparently existing capability gaps and newly emerging needs to the fore, accompanied by the need to replenish European armament stocks for the military aid provided to Ukraine. These are the short-, mid-, and long-term needs that the European defence industry will need to address, offering multiple opportunities for developing and even restructuring EDTIB.

48 The original version of this figure had been introduced at the 'National Visions of the EU Defence Industrial "Toolbox": the Italian and Swedish Cases' webinar organised on 12 January 2024, by Institut de Relations Internationales et Stratégiques, with the participation of Alessandro Marrone (Istituto Affari Internazionali), Lorenzo Scarazzato (Stockholm International Peace Research Institute) and Isabelle Desjeux (Safran Electronics). Minor changes applied by the author.

2.3. Military support to Ukraine

The EU and its Member States together provided over 96 billion dollars in financial, military, humanitarian and refugee assistance during the first year of the war. This included over 30 billion dollars in military assistance for ammunition, air defence systems, fighting vehicles, main battle tanks and drones, as well as military training to 40,000 Ukrainian soldiers by the end of 2023. Breaking a strategic taboo, funds from EPF – worth six billion dollars – were used for procuring arms and ammunition for the first time ever to be handed over to Ukraine. In parallel, 2.2 billion dollars were earmarked to reinforce European defence industry capacities and an additional 535 million dollars for ammunition production capacity, both for producing ammunition for Ukraine and replenishing European stocks.[49]

In addition, EU Member States provided significant direct military aid to Ukraine (see Table 2). Although the data are not fully transparent, open-source data from Oryx provide an estimate of the quantity of equipment handed over to Ukraine in 2022–2023. With more than 10,000 pieces of major arms assets provided to Ukraine internationally over two years, EU Member States are registered to have delivered and pledged more than 4,000 of these, providing most aircraft (100%), tanks (96%) and helicopters (72%), as well as a significant proportion of air defence systems (55%), artillery (53%) and armoured fighting vehicles (33%) by January 2024.

Table 2: Major arms provided for Ukraine by EU Member States as military assistance in 2022–2023.[50]

Major arms	EU Member States			Total international	Verifiable EU ratio
	Delivered	Pledged	Total		
Aircraft	**45**	**58**	**103**	**103**	**100%**
Helicopters*	**44**	**17**	**61**	**85**	**72%**
Tanks	**576**	**249**	**825**	**860**	**96%**

49 European External Action Service, 2024.

50 AFV: armoured fighting vehicle; IFV: infantry fighting vehicle; APC: armoured personnel carrier; MRAP: mine-resistant, ambush-protected vehicle; IMV: infantry mobility vehicle; MLRS: multiple rocket launch systems; SAM: surface-to-air missile.
*: Attack, transport and utility helicopters in total.
**: The total number is unknown as many pledges and deliveries were not publicly declared.
Source of data: Oryx, 2024. All data reflect the situation as of 1 February 2024. The table was compiled by the author.

Major arms	EU Member States			Total international	Verifiable EU ratio
	Delivered	Pledged	Total		
Armoured fighting vehicles total	**1,479**	**1,465**	**2,592**	**7,910**	**33%**
Including: AFV**	40	n. a.	n. a.	160	25%
IFV	374	340	714	900	79%
APC	752	550	1302	2200	59%
MRAP**	82	230	n. a.	1150	min. 27%
IMV	231	345	576	3500	16%
Artillery total	**533**	**81**	**593**	**1,126**	**53%**
Including: Towed artillery	114	31	176	461	38%
Self-propelled artillery	367	50	417	555	75%
MLRS**	52	n. a.	n. a.	110	min. 47%
SAM systems**	**52**	**14**	**66**	**121**	**55%**

This aspect is important for two reasons: on the one hand, major arms, weapons and equipment, as well as ammunition were provided from existing stocks, thus inevitably reducing the readiness and defence capabilities of European countries in the short term, even if we take into consideration that not necessarily most modern equipment had been handed over, but in many cases outdated post-Soviet legacy assets (as these were compatible with the Ukrainian armed forces). However, eventually discarding legacy equipment – particularly in Central and Southeastern Europe – forces these donor countries to acquire new, modern equipment, necessitating extra defence investments for procurement and creating a situation when they can decide whether to buy European or other products.[51] This is a high value gap on the demand side for EDTIB, to be addressed or wasted.

51 It is worth noting that military assistance to Ukraine since 2022 has not been the first incentive aimed at European countries to replace Soviet legacy military assets in their armed forces' inventories. The U.S. European Recapitalization Incentive Program, established in 2018, granted close to 300 million dollars in financial subsidy to countries buying American weapons worth 2.5 billion dollars. This is the same concept that EU and EU Member States would need to follow – bound to a commitment of buying European arms to support EDTIB. See: U.S. Department of State, 2021.

3. Snapshot of European defence investment trends

There are a couple of choices for obtaining data on European defence expenditure trends, such as the Military Expenditures Database of SIPRI or NATO's defence expenditure data; however, for consistency in methodology and comparability of data, we rely only on defence data released by EDA annually. In December 2023, the latest data, focused on defence investment in 2022 and long-term trends between 2005 and 2022.[52] This also provided an opportunity to track the negative effects of the 2008–2009 economic crisis and the turning trend after 2014–2015, as assessed previously in this chapter. However, most defence spending pledges that had been taken as reactions to Russia's repeated aggression were realised in 2023 and as such, could not be included in this overview.

Although there is no legally binding target for individual national defence spending levels for EU Member States, most of them had agreed in the framework of PESCO and/or NATO to increase their defence expenditures in principle (in NATO: towards the 2% of GDP benchmark). As mentioned earlier, strategic drivers are pressuring European countries to strengthen their defences for several reasons, and in many ways, their improved record of defence spending over the past two years is understandable.

As noted by EDA, in 2022, the total defence expenditure of EU-27[53] totalled 240 billion euros, continuing an increasing trend for eight years on a row – since 2015 – and realising a 6% increase in real terms compared to 2021. Compared with the low point of 2014, their total defence expenditure increased by 69 billion euros, or 40% in real terms, but still lagged by 76 billion euros, had they spent at the 2% GDP level (Figure 4). The data also indicate that EU defence spending returned to the pre-crisis (2008–2009) level only in 2019, which translates into a decade of lost investments.

Among defence expenditures, defence investment constitutes the procurement of defence equipment and R&D. In 2022, defence investment registered a 5.9% growth compared to 2021, reaching a total of 58 billion euros, surpassing the 20% agreed benchmark by 10 billion euros in 2022, a positive trend visible since 2018 (Figure 5). As the EDA noted, 20 of 27 Member States fulfilled the 20% benchmark, with 14 countries surpassing 25% and the highest share being 53.5%.

In 2022, Member States allocated 48.6 billion euros for the procurement of new equipment, taking 83.7% of the defence investment expenditure, up by 7% year-on-year, signalling more extensive – or more expensive – investments in defence equipment. Meanwhile, spending on R&D reduced by 1.9% compared to 2021. It is worth noting that 25 Member States spent more than 90% of their defence investment on procurement; the overall trend indicates that these are mostly off-the-shelf procurements from non-EU countries, which has been further reinforced by the current security context, as will be explained in detail later.

52 European Defence Agency, 2023. All data in this subchapter are derived from this source unless noted otherwise.

53 As Denmark ended the opt-out from CSDP, effective July 1, 2022, as a direct consequence of Russia's invasion of Ukraine, Danish defence expenditure data had also been included (unlike in previous years).

Figure 4: EU-27 total defence expenditure (constant 2022 prices) and 2% of GDP guideline[54]

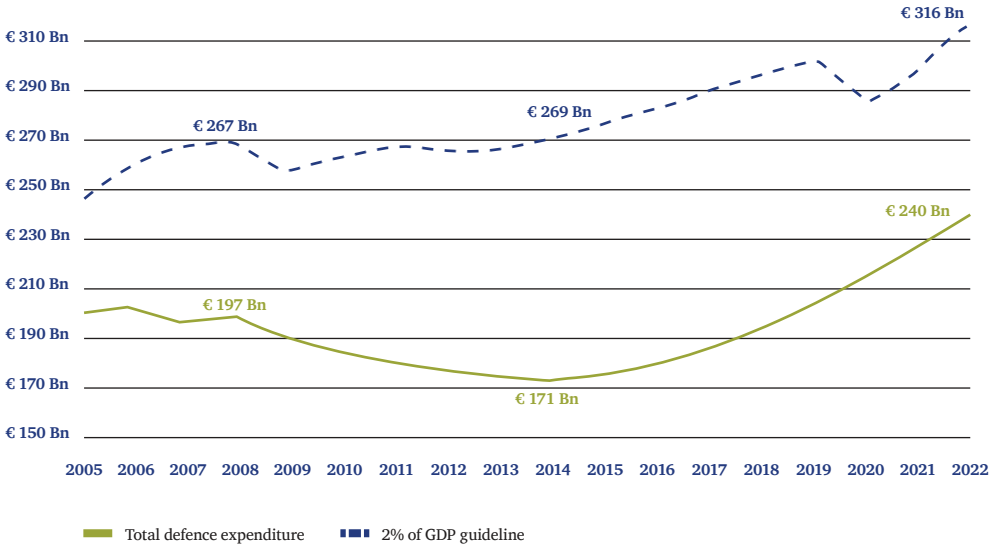
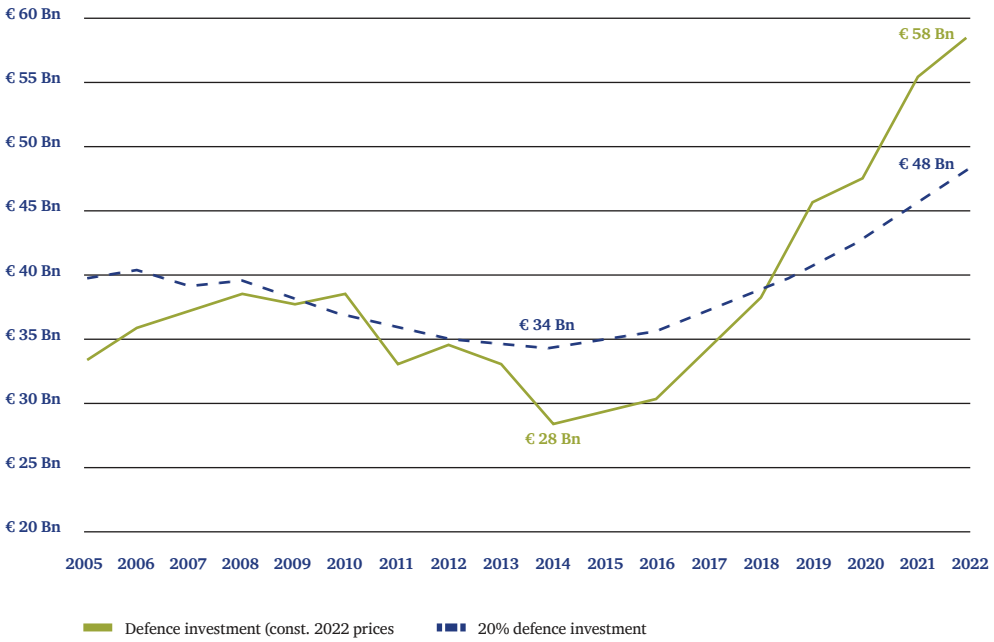


Figure 5: EU-27 total defence investment (constant 2022 prices) and expected 20% defence investment level[55]



54 European Defence Agency, 2023, p. 4.
55 European Defence Agency, 2023, p. 8.

Defence R&D was funded by the remaining 16.3%, or 9.5 billion euros of defence investment in 2022, of which research and technology (R&T) received 3.5 billion euros, a 5.7% year-on-year decrease in real terms, while only two countries fulfilled the 2% benchmark in this field in 2022 and three spent between 1–2% on defence research and technology. This is in stark contrast with the 41% increase from 2020 to 2021.

In sum, we have seen a positive trend regarding the overall financing of defence, driven by the threat perception of a deteriorating and destabilising security environment in the European neighbourhood, both in the east and south. Simultaneously, Member States have a relatively mixed record of long-standing benchmarks regarding how these funds should be used collaboratively, going beyond national R&D, production and procurement.[56] EU Member States allocated more than 20% of their defence investments for equipment procurement (including R&D and R&T), but defence R&T funds remained below the 2% benchmark for total defence spending in 2022. Regarding European collaborative equipment procurement, which should be at least 35% of total equipment spending, EDA could not provide an assessment because procurements were not transparent, with only a few countries providing the data.[57]

Considering that defence expenditures and procurements soared since Russia's 2022 invasion of Ukraine, it is imperative to look beyond EDA data for 2023, which is possible following the announcements of European countries. As Maulny summarised, of the 27 European countries that have released public data on defence (25 EU countries, the United Kingdom and Norway), 25 increased their defence expenditures from 2022 to 2023. In 18 of these 25 countries, the increase was higher than the rate of inflation, resulting in real term growth, while Latvia, the Netherlands, Poland, Slovakia and Slovenia announced increases twice the rate of inflation. Poland announced a 46% (!) nominal increase, while Austria, Baltic countries, Finland and Sweden reported a 20% increase.[58] Notably, the German government created a 100-billion-euro special fund for defence modernisation and financing short-term procurements, to be used until 2025. Based on national data, the equipment expenditure of European countries from 2022 to 2023 increased by 21.5 billion euros, with Germany representing approximately one-third of the total, and Poland providing

56 EU Member States approved four collective benchmarks for defence investment in November 2007 within the EDA Ministerial Steering Board meeting.

57 In 2017, only 7% of R&D (compared to the 20% target) and 17% of procurement (compared to the 35% target) were conducted in a multinational framework; 80% of procurement programmes were national, which is guaranteed by Article 346 of the Lisbon Treaty, allowing Member States to claim that national security can only be guaranteed if procurement is carried out nationally. This is so although it was originally intended to be the "exception" and not the "rule" – but multinational defence industrial cooperation requires (would require) a particularly strong political will. This national attitude is currently being challenged by the incentives to fund capability development, as well as R&D, in multinational frameworks only (PESCO, EDF). European Court of Auditors, 2019, pp. 47–48.

58 Maulny, 2023, p. 5.

more than 15%. By contrast, EU countries' defence investment grew by 8.4 billion euros in the previous year.[59]

Despite the outstanding short-term increase triggered by the strategic shock of the escalating Russo-Ukrainian War, it remains uncertain, how long this drive will last. EDA estimates EU defence spending to rise to 290 billion euros in 2025, but longer-term multi-year defence spending is an exception than a rule among European countries (France and the Netherlands as positive examples); thus, the stability and predictability of defence investments is not guaranteed. It depends on various factors, such as how the war in Ukraine will unfold in 2024–2025, whether there will be an escalation or territorial expansion of the conflict, how European countries assess their military defence capabilities, quantitative and qualitative capability gaps, and financial sustainability of their defence efforts. Lastly, the outcome of the upcoming U.S. elections and certainty of its defence guarantees – at least verbally dependent on Donald Trump's commitment if elected – could have a direct impact on European defence efforts.

Beyond the surge in defence investment, procurements have also been soaring since mid-2022; total equipment acquisitions contracted by European countries from mid-2022 to mid-2023 are estimated to be around 100 billion euros, representing a 21.5 billion-euro increase year-on-year. Maulny's assessment demonstrated that 70–75% of acquisitions had been contracted after Russia's invasion, and 5% were linked to stock replenishments. Acquisitions from outside the EU accounted for 78% of procurement contracts, with the United States alone accounting for 63%.[60] A few examples of high-value acquisitions include 35 F-35A aircrafts (7.9 billion euros) and 60 CH-47 helicopters (8 billion euros) for Germany, and 96 AH 64-E helicopters as well as tanks, armoured vehicles, combat aircraft, artillery, missiles and UAVs (worth 25 billion euros for Poland). While defence procurements have surged since 2022, European defence industrial production has fallen short on capacity and delivery times spanning years, thus pushing off-the-shelf procurements to the forefront of many European countries. As Liang et al. noted, arms companies' efforts to increase production capacity in 2022 were hindered by labour shortages, rising costs and supply chain disruptions.[61] These tensions must be addressed through the development of EDTIB, as discussed in the following sections.

59 Maulny, 2023, p. 6.
60 Maulny, 2023, p. 2.
61 Liang et al., 2023, p. 1.

4. Developing European Defence Industrial and Technological Base in the 2020s

As changing European threat perceptions have prioritised defence, and the strategic shock of Russian aggression pushes forward the realisation of the EU's strategic vision in terms of upgrading military capabilities by providing increased funding, the key questions for the next few years appear to be: what equipment and assets to buy, and from what source? Essentially, how does the demand and supply meet? There is also a tension between short-term priorities, such as replenishing stocks, and long-term goals, such as developing an EDTIB.

4.1. The basic tenets of arms procurements and arms industry development

There are fundamental requirements for adequately equipping defence forces. As Uttley summarised:

> Three perennial procurement challenges emerge from the primary objective of ensuring armed forces are equipped to achieve national security and foreign policy objectives. The first is "what equipment to buy" to minimize the risk of their national armed forces becoming inferior relative to actual or potential rivals. The second challenge for states is "where to buy equipment from"; states need to create and secure dependable supply chains that enable them to maintain "operational sovereignty" over the use of their military equipment. The third challenge for governments is "how to buy military capability" to ensure the timely procurement of new equipment that meets the performance requirements of the armed forces at fair and reasonable prices.[62]

Accordingly, there are four procurement goals for any State:[63] (a) ensure that the national armed services are equipped with state-of-the-art military systems; (b) obtain an appropriate degree of national autonomy – or "security of supply" – over the use, upgradation and replacement of the weapons systems acquired by their armed forces;[64] (c) realise "indirect" national economic, technological, industrial and

62 Uttley, 2018, p. 73.

63 Uttley, 2018, p. 75.

64 As Uttley points out, 'All states, in the abstract, strive for national self-sufficiency through the creation or retention of indigenous defense-industrial capacity capable of domestic weapons research, development and production. In practice, evidence suggests that states with existing indigenous defense industries have sought to restrict their purchasing of strategically important military equipment and sub-systems to domestic suppliers on "security of supply" grounds. Correspondingly, states with limited or non-existent defense industrial capabilities have sought to minimize their dependence on non-national suppliers when importing weapons by insisting on local production and development rights ("offsets") in arms transfer agreements.' Uttley, 2018, p. 75.

employment benefits arising from their defence procurement expenditure; (d) secure "value-for-money" when choosing between alternative weapons systems available from domestic and non-domestic suppliers.

In European countries, these goals translate into providing fifth generation fighter/multirole aircraft, air-to-air refuelling, strategic airlifts, drone forces, satellite communications that underpin intelligence, surveillance, target acquisition and reconnaissance capabilities, air and missile defence, modern surface naval combatants and submarine forces, as well as the next generation of land forces, such as the main battle tank, armoured fighting vehicles and long-range precision artillery. To provide several of these assets, probative European collaborative programmes have R&D as well as production. These include the Future Combat Air System and Tempest programmes, NH-90 multirole helicopter, A400M medium transport aircraft, European Medium Altitude Long Endurance Remotely Piloted Aircraft System (Eurodrone), Galileo and GOVSATCOM satellite positioning and communication systems, TWISTER missile defence system and Main Ground Combat System. These programmes offer opportunities for multinational collaboration, building on national defence industrial champions, thus pointing to the gradual transformation of EDTIB, making it efficient, competitive and offering cutting-edge products in the long term.

Practically, these goals are inherently conflicting. The goal of procuring state-of-the-art military equipment (Goal 1) may fuel the destabilisation of regional arms races, contradicting the fundamental aim of Member States conducting armed forces development, namely ensuring higher levels of security. Pursuing "security of supply" in procurements (Goal 2) by prioritising domestic defence industries in development and production may conflict with "value-for-money" imperatives (Goal 4) to buy cheaper foreign products available in shorter timescales off-the-shelf. Similarly, seeking "indirect" national benefits (Goal 3) by engaging with domestic defence firms may contradict economic efficiency (Goal 4) pursued by procurements from international markets, taking advantage of open competition.[65] These contradictions remain relevant in the 2020s, when the current, perhaps only short-term, enabling conditions offer a chance to reform and empower the European defence industry.

Considering these influencing factors, States can rely on alternative weapons acquisition strategies, ranging from self-sufficiency through collaboration to licenced production/co-production and off-the-shelf procurement (Figure 6).

65 Uttley, 2018, pp. 76–77.

Figure 6: Alternative national strategies of weapons acquisitions[66]

Self-sufficiency	Collaboration	Licenced production / Co-production	Off-the-shelf procurement
Indigenous research, development and production	Joint research, development and production	No indigenous research and development Indigenous manufacturing	No indigenous development or production

Self-sufficiency ⟷ *Technological dependence on other States*

These strategies can be modelled on a spectrum between self-sufficiency and off-the-shelf procurement, in order of decreasing national independence and domestic national industrial activity. Self-sufficiency is a strategy followed by the most advanced and capable Tier-1 defence economies in particularly important, technologically-advanced sectors, such as space, aviation and nuclear technology.[67] International collaborations can build on the pooling and sharing of R&D and production costs of new weapons systems with other advanced state producers.[68] Licenced production/co-production makes it possible to avoid domestic research and development because manufacturing technologies designed elsewhere are used under a licence in domestic production.[69] The strategy that is most dependent on other producers is off-the-shelf procurement, which eludes domestic R&D and production costs by importing complete weapons systems from abroad. However, as many examples from the past two decades' procurement and production practices demonstrate, "security of supply" and considerations favouring national defence industrial base have been predominating the choices between procurement strategies as opposed to non-national sources of equipment supply.

As mentioned in EDA annual assessments,[70] this limits the extent of cooperation and internationalisation of defence industrial supply, including R&D. Although technically, defence procurements are subject to the common provisions of European procurement law, as provided in the Treaty on the Functioning of the European Union (TFEU), Directive 2009/43/EC and Directive 2009/81/EC, Member States regularly refer to the exception provided by Article 346 TFEU, permitting them to take necessary measures to protect their essential security interests, that is, allowing them to not abide by the Common European Procurement Law. Consequently, the

66 Dorman et al., 2015, p. 25.
67 Such as Saab Gripen or Dassault Rafale fighter aircraft being national air force models sold to foreign customers as well.
68 Such as Eurofighter Typhoon produced in collaboration with BAE Systems, Airbus, Alenia Aermacchi and DASA within Eurofighter GmbH.
69 Such as the assembly and later the production of Lynx infantry fighting vehicles in Hungary.
70 European Defence Agency, 2023.

costs of procuring "non-European" in defence was estimated to range between 26 and 130 billion euros already in 2013.[71] Ten years later, the European Parliamentary Research Service estimated that the potential gains of "choosing European" in the 2020s could be between 24.4 billion and 75.5 billion euros annually (Table 3).[72]

Table 3: The breakdown of possible financial gains through more European cooperation in defence[73]

Main category		**Moderate approach** *(billion euros)*	**Ambitious approach** *(billion euros)*
1. Common capacity not created otherwise	Deployable troops	–	32
	R&D	–	6.4
2. Efficiency gains	Efficiency gains in industrial production	14.2	14.2
	Efficiency gains in land forces	1.3	1.3
	Efficiency gains in air force	0.2	0.2
	Efficiency gains in navy	0.5	0.5
	Efficiency gains in logistical support	0.4	0.4
3. Lower administrative costs	Procurement	–	12.7
4. Integration of externalities	Savings on offsets	7.8	7.8
Total		**24.4**	**75.5**

4.2. EDTIB's prime actors' place in the global defence industry

Although defence industrial collaboration in R&D and production, as well as joint procurement, would be a logical step to efficiently use economies of scale, to share resources and know-how, thus boosting competitiveness and the technological edge of European products internationally, such initiatives have only been a limited choice among European countries in the past decades. This can be attributed

71 Ballester, 2013, p. 8.
72 European Parliamentary Research Service, 2023, p. 314.
73 European Parliamentary Research Service, 2023, p. 314.

to national – economic, technological and often political – interests being contradictory, especially because EDTIB is largely fragmented and comprises various producers with diverse levels of technological advancement, capitalisation, capabilities in production, know-how and skilled employees, as well as relying on diverse supply chains.

Bitzinger classified States into a three-tier hierarchy in terms of their indigenous capacity to develop and produce advanced weapons.[74] The "First Tier" of arms-producing States, including the United States, United Kingdom, France, Germany, Italy, Israel, Russia – and today China – possess the world's largest and most technologically-advanced defence industries. The domestic defence industries in these States collectively account for approximately 90% of global armament production. They dominate the global defence R&D process and have the resources and capacity to sustain self-sufficiency across some or all weapons development and production sectors. The "Second Tier" comprises a diverse range of countries. Some possess small but sophisticated arms industries (e.g. Austria, Canada, Sweden), while others are developing or newly industrialised countries (e.g. Brazil, South Africa, Republic of Korea, Turkey and gradually Poland). India currently fits into the group of Great Powers, having a large, broad-based defence industry but lacking domestic capacity to develop and produce sophisticated conventional arms. The "Third Tier" includes States that possess limited and low-technology arms-production capability, such as Egypt, Mexico and Nigeria. The remaining States in the international system lack the means to develop or produce weapons systems, therefore rely on arms imports and other forms of inward technology transfer to meet their military equipment requirements.

EU Member States comprise countries from all tiers with varying degrees of the ability to advocate their industrial interests. According to Lian et al., 26 EU arms companies were among the Top 100 arms producing and military services companies in 2022, with their combined arms revenue at 121 billion dollars. Among them, a U.K.-based company (BAE Systems) figured in the Top 10, along with six British, five French, four German, three trans-European, two Italian and other companies (Table 3). Trans-European companies included Airbus (ranked 14th, with arms revenues at 12.1 billion dollars), MBDA (32nd, 4.4 billion dollars) and KNDS (44th, 3.2 billion dollars). In comparison, 42 American (302.6 billion dollars), 8 Chinese (108 billion dollars) and 2 Russian (20.8 billion dollars) companies were listed in the Top 100, signalling strong American dominance. The most successful portfolios of European companies include air defence systems, anti-ballistic missile systems, armoured vehicles and ammunition.[75]

74 Bitzinger, 2003, pp. 6–7, current updates added by the author.
75 Liang et al., 2023, pp. 9–11.

Table 4: Top EU defence companies by revenue in 2022[76]

Company	Country	Revenue (billion USD)*	Global ranking
BAE Systems	United Kingdom	26.9	6.
Leonardo	Italy	12.47	13.
Airbus	Trans-European	12.09	14.
Thales	France	9.42	17.
Dassault Aviation	France	5.07	23.
Rolls-Royce	United Kingdom	4.93	25.
Rheinmetall	Germany	4.55	28.
Naval Group	France	4.53	29.
MBDA	Trans-European	4.38	32.
Safran	France	4.2	34.

European defence industrial production capacities are unevenly distributed among Member States; the largest ones account for approximately 80%, with an estimated turnover of 100+ billion euros. A relatively fewer number of large companies (a few dozen) and over 2,000 small-and-medium enterprises (SMEs) in the production chain form the backbone of this sector.[77] EDA estimated that in 2021, 196,000 highly-skilled people were directly employed in the industry, indirectly supporting over 315, 000 jobs.[78] European SMEs active in the defence and security industry are typically local-based, nationally linked at some point in the large corporate supply chain, and highly dependent, even vulnerable, to economic-financing problems. This group of small businesses was understandably severely affected by the resource constraints of the first half of the 2010s; therefore, it must be ensured that they remain viable within national and EU frameworks and resources in the 2020s. Technological know-how of the entire production chain is clearly of strategic importance, and these building blocks are needed if the EU is to secure strategic autonomy at any time in the future.

For decades, this defence industrial base has been leading the world in terms of its R&D potential and manufacturing capacity, whether for military or dual-use

76 Source of data: Ibid. The table was compiled by the author.
*: Revenues from arms production and sales in 2022.
77 European Court of Auditors, 2019, p. 43.
78 European Parliament, 2023.

technologies. In addition, the activities of the largest defence industry companies are global in scope – an approach that clearly shows a loss of ground for emerging competitors. While these companies accounted for nearly 30% of the global share after the turn of the millennium, by the end of the 2010s, their share had fallen below 25%, while the share of non-Western (non-EU, non-U.S.) defence industrial companies increased from 9% to 19%.[79] As the largest customers of European defence industrial products are EU Member States, their budgetary constraints directly affect their market opportunities. This highlights that both the demand and supply sides are vulnerable – and can offset their ability to compete in international arms trade. Given that the results of defence R&D can be measured in decades, while the present results are ensured by decisions made decades ago, it is important to consider the severe resource cuts in this area in the 2010s, from which the sector has yet to recover.

Moreover, the Russo-Ukrainian War revealed further shortcomings for the EDTIB in terms of meeting the increased short-term demand for arms and military stocks, particularly for ammunition and air defence missiles. The past two years have raised questions about the European industry's ability to support Ukraine militarily at scale and speed, and its ability to recapitalise forces in NATO and the EU.[80] For example, BAE Systems estimated that restarting the production of M777 howitzers would take 30–36 months; Rheinmetall deemed 8–12 months necessary for the production of specialised steel for tank armour, while the delivery time of unguided 155 mm artillery shells was 10–20 months, and 24–36 months for guided shells in 2022. It is estimated that in high-intensity conflict, the United Kingdom's ammunition stocks would last around eight days, while Bundeswehr would run out of ammunition somewhere between a few hours and a few days, as they only count on stocks of 20,000 155 mm artillery shells – enough for less than three days of high-intensity combat in Ukraine. In 2022, France produced an equivalent of these shells for a week of fire during World War II.[81]

4.3. Constraints and opportunities for EDTIB in the 2020s

An overview of the European defence industrial sectors reveals that aerospace is characterised by a relatively high level of cooperation and integration compared with other sectors. In recent decades, a significant number of bilateral to multilateral collaborative programmes have taken place in the EU, such as the A400M transport aircraft, NH90 multirole helicopter, Eurocopter Tiger attack helicopter, Eurofighter Typhoon fighter aircraft, MALE RPAS drone and the Meteor air-to-air missile. However, programme duplications have occurred, for example,

79 European Court of Auditors, 2019, pp. 49–50.
80 Aries, Giegerich and Lawrenson, 2023, p. 7.
81 Data from Aries, Giegerich and Lawrenson, 2023, p. 9; Calcara, Gilli and Gilli, 2023, p. 635.

fighter aircraft such as Rafale, Gripen and Eurofighter.[82] The European aerospace sector can deliver advanced military capabilities and cutting-edge technologies independently, such as combat aircraft, helicopters, missiles, strategic airlift and tanker aircraft. This branch is comparatively well positioned in the global market, with top players sustaining strong export records, such as Rafale and Eurofighter aircraft, Eurocopter and various types of MBDA missiles. However, the market continues to be dominated by leading American companies, such as Lockheed Martin and Boeing, returning to European markets and taking a significant share of the F-35 Joint Strike Fighter after the decades-long success of F-16 variants.[83] Meanwhile, there are certain shortcomings in air and missile defences: despite existing – though partial – European solutions such as SAMP/T, and IRIS-T air-to-air missiles, the comprehensive European Sky Shield Initiative also builds Patriot for long-range and Arrow 3 for very-long-range missile defence (sidelining SAMP/T). The aerospace sector is highly R&D-intensive (up to 30% of the total cost of a combat aircraft) and is strongly interconnected with civilian aviation. Therefore, with a few exceptions, such as BAE Systems, MBDA and Saab, leading companies are involved in dual-use activities and are not fully dependent on the defence sector.[84]

The land armament industry is less concentrated than the aerospace segment. Here, the main integrators are concentrated in the "Letter of Intent" group[85]: France, Germany, Italy, Spain, Sweden and the United Kingdom, while SMEs play a substantial role as subcontractors and specialised product suppliers operating in niche markets. Compared to the aerospace industry, the land armament industry is relatively more defence-dependent but less R&D-intensive, with typically less than 15% associated with R&D costs.[86] In addition, there are fewer dual-use opportunities. Collaborative projects have been very limited, such as the German–Dutch armoured fighting vehicle Boxer or the Krauss-Maffei Wegmann–Nexter merger into KNDS, bringing about an important step in industrial consolidation. The sector is characterised by the duplication of capabilities along national borders.

82 Research costs and the cost effectiveness of production greatly determine competitiveness. The research costs of the Eurofighter were said to be 19.48 billion euros, surpassing even that of F-35 with 19.34 billion euros. However, for this similar R&D investment 707 Eurofighters and 3003 F-35s were envisaged to be produced. Briani, 2013, p. 16.

83 Currently there are 142 F-35 variants in service in Europe (10 in Denmark, 26 in Italy, 34 in the Netherlands in the EU, plus 40 in Norway, 32 in the United Kingdom). Additional 64 F-35s have been contracted by Finland, 34 by Belgium, 32 by Poland, 35 by Germany, 24 by the Czech Republic and 36 by Switzerland. The procurement of further 40 aircraft is being negotiated with Greece.

84 European Court of Auditors, 2019, p. 68.

85 The "Letter of Intent" group was formed in 2000 to create the political and legal frameworks necessary to facilitate industrial restructuring to promote a more competitive and robust EDTIB in the global defence market. This aim should be realised through tackling challenges in six broad areas: security of supply, transfer/export procedures, security of information, research, treatment of technical information and harmonisation of military requirements.

86 European Court of Auditors, 2019, p. 68.

Currently, there are 49 design families of armoured fighting vehicles and 11 design families of tanks in operation in the EU. Opportunities for further collaboration exist with the European Main Battle Tank and a future artillery system developed by France and Germany, as the sector can design, manufacture, upgrade and support key military capabilities for land warfare. These also include armoured fighting vehicles, ammunition, precision munitions, artillery systems and missile launchers. Producers perform strongly in global exports, like the Leopard main battle tank and various armoured vehicles. However, competition in the global market involves ever more players than traditional Tier-1 manufacturers (such as the United States, Russia, Israel and South Korea), as Tier-2 countries (Turkey and India) also develop their indigenous defence industries. The competitiveness of the EU industry is affected by the relatively small size of the main European companies compared to American companies. The Russo-Ukrainian War also revealed shortcomings in European production capacities in several areas of the land domain, such as ammunition production, anti-tank-guided missiles, artillery and demining equipment.

The European naval industry is concentrated around six major companies that serve as prime contractors and system integrators. These can design, integrate and produce an entire range of key capabilities, from ships to almost all core systems and components up to, aircraft carriers and nuclear-capable submarines. Major producers rely on diverse supply chains comprising many specialised suppliers, and there is no dependency on non-EU countries for critical systems, even after Brexit. This sector is highly competitive in international markets, especially in high value-added segments such as submarines, destroyers and frigates. However, the naval sector remained organised along national borders, with 60–80% of materials, components and systems sourced at the national level by prime contractors. This increased to 95% when taking into account EU cooperation in the supply chain. Experience with EU collaborative projects has been limited in the naval sector, and mainly took place on a bilateral basis, such as the Fromme multipurpose frigate developed by France and Germany. With growing competition from China and South Korea, the naval sector is increasingly dependent on exports.[87]

The SWOT analysis of EDTIB summarises the constraints and opportunities for the 2020s (Table 5).

87 European Court of Auditors, 2019, p. 68.

Table 5: SWOT analysis of EDTIB[88]

Strengths	**Weaknesses**
– Presence of European leaders in global markets – Capacity to design and produce a wide range of military products in aerospace, land, naval and electronic segments – Experience in multinational cooperation (particularly in the aerospace sector) – Highly skilled workforce	– Fragmented defence market with excess capacity in certain areas, duplications and missed economies of scale – *Limited production capacities in other areas (ammunition, missile technology, air defence, land vehicles)* – Increasing costs of defence equipment and systems – Relatively low-level of R&D expenditures – Lack of collaborative defence procurements and R&D (*initially addressed by EDF and EDIRPA, later by EDIP*) – Divergence in EU Member States' export policies – Limited access to cross-border markets within the EU, in particular for SMEs (*addressed by PESCO and EDF*)
Opportunities	**Threats**
– Growth in global and European military expenditures – Large-scale demand from European countries both for supporting Ukraine, replenishing their own stocks and – Momentum for EU defence cooperation supported by (*most*) Member States (*and EU institutions*) – Launch of large new collaborative programs (FCAS, Euro drone MALE, European Main Battle Tank, *Tempest*, *European Sky Shield Initiative*) – Potential for rationalisation and restructuring, particularly in the land and naval sectors – Dual-use technologies and growing interaction with the civilian sector	– Competition from traditional and emerging competitors – Loss of innovative capacity and technological superiority, hindering global competitiveness – Security of supply with increased dependency on international and complex supply chains – No preference for using EU suppliers by member states – High entry barriers in non-EU market

88 European Court of Auditors, 2019, p. 69. Emphasis in italics, signalling additions, were added by the author.

5. Conclusions: squaring the circle between short-term readiness and long-term innovation

As European countries adapt their procurement plans to move from the previous crisis management phase dominated by asymmetric warfare against small States and non-State actors to an era of strategic competition and potential conflict against peer adversaries, there are several structural issues that EDTIB must address. On the demand side, there is a short-term request for the replenishment of state-of-the-art arms and ammunition stocks, as well as for procuring new modern equipment to replace legacy assets provided for Ukraine in 2022–2023. Second, for the mid-term, the ongoing weapons development programmes and production contracts must be realised, sometimes even upgraded in numbers and/or quality, reflecting the technological lessons learnt from the Russo-Ukrainian War. Third, in the long-term, investment-intensive research and development, and innovation in emerging and disruptive technologies, such as autonomous systems, AI, quantum computing, hypersonic systems, space, novel materials and manufacturing, energy and propulsion, next-generation communications systems, biotechnologies and human enhancements need to be addressed by EDTIB not only to keep pace with global competitors, but also to maintain competitiveness and develop a new technological edge.

To meet these demands on the supply side, the defence industry reacted with the extension of working hours, introducing new shifts to increase production levels for existing lines, and started to invest in and introduce further production capacities, such as opening new lines, extending facilities, even building new arms factories in Europe (planned to be extended soon to Ukraine), and further acquisitions and mergers. New major investments may begin to yield results within a few years, as shown by the protracted introduction of extra ammunition production capacity since 2022. The EU also attempts to live up to the changed circumstances, introduce new applications for existing programmes (EDF, EPF) and establish new incentives (ASAP, EDIRPA, EDIP). The EDIS, with all supporting mechanisms – and hopefully also building upon the strong commitment of Member States – should enable the EU to address these long-term issues.

However, when current incentives for short-term defence procurement and readiness collide with long-term structural investment, consolidation and innovation, there is an inevitable trade-off. Limited resources make this balancing a challenge, independent of the actual outcome of the Russo-Ukrainian War, because resources are now being committed to mid-to-long-term contracts. While EDIRPA only encourages consolidation of the demand side, EDIP should focus on supporting the supply side by creating a framework favourable to the development of the European defence industry, enabling it to produce more, better and faster.[89]

89 Schnitzler, 2023, p. 3.

References

Anderson, J.J., Biscop, S., Giegerich, B., Mölling, C., Tardy, Th. (2016) *Envisioning European defence. Five futures*. Chaillot Paper No. 137, Paris: EUISS; https://doi.org/10.2815/83614.

Andersson, J.J., Cramer, C.S. (2023) *EUISS Yearbook of European Security 2023*. Luxembourg: Publications Office of the European Union; https://doi.org/10.2815/168634.

Aries, H., Giegerich. B., Lawrenson, T. (2023) 'The guns of Europe: Defence-industrial challenges in a time of war', *Survival*, 65(3), pp. 7–24; https://doi.org/10.1080/00396338.2023.2218716.

Ballester, B. (2013) *The Cost of non-Europe in Common Security and Defense Policy*, Brussels: European Union Research Service; https://doi.org/10.2861/28157.

Barrie, D., Béraud-Sudreau, L., Boyd, H., Childs, N., Giegerich, B., Hackett, J., Nouwens, M. (2020) *European defence policy in an era of renewed great-power competition*. IISS – Hanns Seidel Foundation. [Online]. Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/european-defence-policy-in-an-era-of-renewed-great-power-competition---iiss-research-report.pdf (Accessed: 10 December 2023).

Bergmann, M., Besch, S. (2023) 'Why European defense still depends on America', *Foreign Affairs*, 7 March 2023. [Online]. Available at: https://www.foreignaffairs.com/ukraine/why-european-defense-still-depends-america (Accessed: 10 December 2023).

Bergmann, M., Svendsen, O. (2023) *Transforming European Defense. A new focus on integration*. Washington, DC: CSIS. [Online]. Available at: https://www.csis.org/analysis/transforming-european-defense-new-focus-integration (Accessed: 10 December 2023).

Bitzinger, R. (2003) 'Towards a brave new arms industry?', *The Adelphi Papers,* 43(356), pp. 63–79; https://doi.org/10.1080/714027876.

Briani, V. (2013) *The cost of non-Europe in the defense field*. Rome: Centre for Studies on Federalism – IAI. [Online]. Available at: https://www.iai.it/sites/default/files/CSF-IAI_noneuropedefence_april2013.pdf (Accessed: 10 December 2023).

Calcara, A., Gilli, A., Gilli, M. (2023) 'Short-term readiness, long-term innovation: the European defense industry in turbulent times', *Defence Studies*, 23(4), pp. 626–643; https://doi.org/10.1080/14702436.2023.2277439.

Čižik, T. (2020) 'Security perception and security policy of the Slovak Republic, 1993–2018', *Defense and Security Analysis*, 37(1), pp. 23–37; https://doi.org/10.1080/14751798.2020.1831228.

Commijs, K. (2020) 'Kabinet doet te weinig om kernwapenverdrag te redden' [Cabinet does too little to save nuclear arms treaty], *Trouw*, 31 January 2020. [Online]. Available at: https://www.trouw.nl/nieuws/kabinet-doet-te-weinig-om-kernwapenverdrag-te-redden~b39d3ec4/ (Accessed: 10 December 2023).

Council of the European Union (2013) 'Conclusions, 19/20 December 2013', 20 December. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-217-2013-INIT/en/pdf (Accessed: 10 December 2023).

Council of the European Union (2021) 'Council Conclusions on Security and Defense, Outcome of Proceedings', 10 May. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-8396-2021-INIT/en/pdf (Accessed: 10 December 2023).

Council of the European Union (2022a) 'A Strategic Compass for Security and Defense', 21 March. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf (Accessed: 10 December 2023).

Council of the European Union (2022b) 'Informal meeting of the Heads of State and Government – Versailles Declaration', 11 March. [Online]. Available at: https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf (Accessed: 10 December 2023).

Council of the European Union (2024) *European Peace Facility*. [Online]. Available at: https://www.consilium.europa.eu/en/policies/european-peace-facility/ (Accessed: 30 January 2024).

Csernatoni, R. (2021) *The EU's Defense Ambitions: Understanding the Emergence of a European Defense Technological and Industrial Complex*. Brussels: Carnegie Europe. [Online]. Available at: https://carnegieendowment.org/research/2021/12/the-eus-defense-ambitions-understanding-the-emergence-of-a-european-defense-technological-and-industrial-complex?lang=en&center=europe (Accessed: 10 December 2023).

Csiki, T. (2014) 'Az Európai Tanács közös biztonság- és védelempolitikai csúcstalálkozójának háttere és eredményének értékelése' [The background and analysis of the EU Council summit on common security and defense policy], *Nemzet és Biztonság – Biztonságpolitikai Szemle*, 7(1), pp. 48–63.

Csiki, T., Tálas, P., Varga, G. (2014) 'A NATO walesi csúcstalálkozójának napirendje és értékelése' [The agenda and analysis of NATO's Wales summit], *Nemzet és Biztonság – Biztonságpolitikai Szemle*, 7(2), pp. 112–128.

Dorman, A., Uttley, M., Wilkinson, B. (2015) *A benefit, not a burden.* King's Policy Institute Paper, London: King's College London.

European Commission (2022a) 'Commission contribution to European defense' COM(2022) 60 final, Strasbourg, 15 February. [Online]. Available at: https://commission.europa.eu/document/download/d53b0f4f-939f-4044-ab16-e8fc44d35b84_en?filename=com_2022_60_1_en_act_contribution_european_defence.pdf (Accessed: 10 December 2023).

European Commission (2022b) 'Defense Investment Gaps Analysis and Way Forward' JOIN(2022) 24 final, Brussels, 18 May. [Online]. Available at: https://commission.europa.eu/system/files/2022-05/join_2022_24_1_en_annexe_autre_acte_conjoint_cp_part1_v1.pdf (Accessed: 10 December 2023).

European Court of Auditors (2019) 'European Defence, Review No. 09.', 22 March. [Online]. Available at: https://www.eca.europa.eu/lists/ecadocuments/rew19_09/rew_eu-defence_en.pdf (Accessed: 1 February 2024).

European Defense Agency (2020) '2020 CARD Report – Executive Summary'. [Online]. Available at: https://www.eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf (Accessed: 10 December 2023).

European Defense Agency (2022) '2022 Coordinated Annual Review on Defence Report', 16 November. [Online]. Available at: https://eda.europa.eu/docs/default-source/eda-publications/2022-card-report.pdf (Accessed: 10 December 2023).

European Defense Agency (2023) 'Defense Data 2022. Key findings and analysis', 29 November. [Online]. Available at: https://eda.europa.eu/docs/default-source/brochures/2022-eda_defencedata_web.pdf (Accessed: 10 December 2023).

European External Action Service (2022) *A Strategic Compass for Security and Defense*. [Online]. Available at: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf (Accessed: 10 December 2023).

European External Action Service (2024) 'EU Assistance to Ukraine (in U.S. Dollars)', 24 April. [Online]. Available at: https://www.eeas.europa.eu/delegations/united-states-america/eu-assistance-ukraine-us-dollars_en? (Accessed: 10 December 2023).

European Investment Bank (2022) 'The EIB continues its support to the EU's Security and Defense Agenda', 10 March 2022. [Online]. Available at: https://www.eib.org/en/press/all/2022-123-the-eib-continues-its-support-to-the-eu-s-security-and-defence-agenda (Accessed: 10 December 2023).

European Investment Bank (2023) 'EIB pledges record funding for Europe's security infrastructure, vows more support for Ukraine', 16 June 2023. [Online]. Available at: https://www.eib.org/en/press/all/2023-227-eib-pledges-record-funding-for-europe-s-security-infrastructure-vows-more-support-for-ukraine (Accessed: 10 December 2023).

European Parliament (2023) 'Reinforcing the European defense industry', June 2023. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/749805/EPRS_BRI(2023)749805_EN.pdf (Accessed: 10 December 2023).

European Parliamentary Research Service (2023) 'Increasing European added value in an age of global challenges. Mapping the costs of non-Europe (2022-2032)', February 2023. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/734690/EPRS_STU(2023)734690_EN.pdf (Accessed: 10 December 2023).

Fiott, D. (2023) 'In every crisis an opportunity? European Union integration in defense and the War on Ukraine', *Journal of European Integration*, 45(3), pp. 447–462; https://doi.org/10.1080/07036337.2023.2183395.

Fiott, D., (2024) *The EU Defense Industrial Strategy: Some preliminary reflections*. [Online]. Available at: https://danielfiott.com/2023/10/21/the-eu-defence-industrial-strategy-some-preliminary-reflections/ (Accessed: 10 December 2023).

IISS (2023) *Military Balance+ database*. [Online]. Available at: https://milbalplus.iiss.org/default.aspx? (Accessed: 10 December 2023).

Karsenti, M. (2023) 'Armement français: "Notre outil industriel ressemble plus à de l'artisanat de luxe qu'à une industrie de défense"' [French armament: "Our industrial base is more like a luxury craft industry than a defense industry"], *Marianne*, 23 February 2023. [Online]. Available at: https://www.marianne.net/societe/defense/armement-francais-notre-outil-industriel-ressemble-plus-a-de-lartisanat-de-luxe-qua-une-industrie-de-defense (Accessed: 10 December 2023).

Kříž, Z. (2020) 'The security perception and security policy of the Czech Republic, 1993–2018', *Defense and Security Analysis*, 37(1), pp. 38–52; https://doi.org/10.1080/14751798.2020.1831231.

Liang, X., Scarazzato, L., Béraud-Sudreau, L., Tian, N., Lopes-Da Silva, D., Choi, Y., Sild, E.-K. (2023) 'The SIPRI Top 100 arms-producing and military service companies, 2022', *SIPRI Fact Sheet*, December 2023. [Online]. Available at: https://www.sipri.org/sites/default/files/2023-11/fs_2312_top_100_2022.pdf (Accessed: 20 December 2023).

Maulny, J.-P. (2023) 'The impact of the war in Ukraine on the European defense market', *Institute de Relations Internationales et Stratégiques*, September 2023. [Online]. Available at: https://www.iris-france.org/wp-content/uploads/2023/09/19_ProgEuropeIndusDef_JPMaulny.pdf (Accessed: 10 December 2023).

Mölling, C., Brune, S. (2011) *The Impact of the Financial Crisis on European Defence*. Brussels: European Parliament. [Online]. Available at: https://www.europarl.europa.eu/document/activities/cont/201106/20110623ATT22404/20110623ATT22404EN.pdf (Accessed: 10 December 2023).

Nádudvari, A. (2020) 'Az európai védelmi kezdeményezések törésvonalai' [The fault lines in European defense initiatives], *Nemzet és Biztonság – Biztonságpolitikai Szemle*, 13(1), pp. 111–131; https://doi.org/10.32576/nb.2020.1.7.

NATO (2023) 'Madrid Summit Declaration' *Press Release*, 22 June 2022. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_196951.htm (Accessed: 10 December 2023).

Oryx (2024) 'Answering the call: Heavy weaponry supplied to Ukraine', 11 April 2022. [Online]. Available at: https://www.oryxspioenkop.com/2022/04/answering-call-heavy-weaponry-supplied.html (Accessed: 01 February 2024).

Palczewska, M. (2020) 'The security perception and security policy of Poland, 1989–2017', *Defense and Security Analysis*, 37(1), pp. 80–95; https://doi.org/10.1080/14751798.2020.1831237.

Sabatino, E., Fiott, D., Zandee, D., Mölling, C., Major, C., Maulny, J., Keohane, D., Moro, D. (2020) *The Quest for European Strategic Autonomy – A Collective Reflection*. IAI. [Online]. Available at: https://www.iai.it/sites/default/files/iai2022.pdf (Accessed: 10 December 2023).

Sarcinschi, A. (2020) 'Security perception and security policy in Romania since the 1989 Revolution', *Defense and Security Analysis*, 37(1), pp. 96–113; https://doi.org/10.1080/14751798.2020.1831239.

Schnitzler, G. (2023) *EDIRPA/EDIP: Risks and opportunities of future joint procurement incentives for the European defense market*. ARES Policy Paper No. 81.

SIPRI (2023) *SIPRI Military Expenditure Database*. [Online]. Available at: https://www.sipri.org/databases/milex (Accessed: 10 December 2023).

Uttley, M. (2018) 'Defence procurement' in Galbreath, D.J., Deni, J.R. (eds.) *Routledge Handbook of Defence Studies*. 1st edn. London: Routledge, pp. 72–86; https://doi.org/10.4324/9781315650463-7.

U.S. Department of State (2021) 'European Recapitalization Incentive Program (ERIP)', 6 December. [Online]. Available at: https://www.state.gov/european-recapitalization-incentive-program-erip/ (Accessed: 10 December 2023).

Wall, C., Christianson, J. (2023) 'Europe's missing piece: The case for air domain enablers', *CSIS Briefs*, April 2023. [Online]. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230417_Wall_European_Enablers.pdf? (Accessed: 10 December 2023).

Zubascu, F. (2024) 'Horizon Europe budget to be cut by €2.1B, as defense research gets a €1.5B boost', *Science|Business*, 1 February 2024. [Online]. Available at: https://sciencebusiness.net/news/horizon-europe/horizon-europe-budget-be-cut-eu21b-defence-research-gets-eu15b-boost (Accessed: 1 February 2024).

Chapter 3

Emerging and Innovative Military Technologies in the EU Member States: Background and Issues

Andrzej Pawlikowski

Abstract

This chapter explores the evolving landscape of military technologies in the European Union (EU) the member states, covering its background, trends, and challenges. Rapid technological advancements have shaped military capabilities, requiring a comprehensive understanding by policymakers, defence analysts, and scholars. This historical overview emphasises the collaborative efforts and the impact of geopolitical shifts on defence strategies. The chapter examines emerging technologies such as artificial intelligence (AI), autonomous systems, cyber capabilities, and space-based innovations, illustrating their integration into military operations through case studies. Ethical, legal, and security issues are analysed, including consideration of autonomous weapons, cyber warfare legal frameworks, and proliferation risks. The chapter also examines standardisation challenges across the EU, and also rivalry between the U.S., China, and Russia. The impacts on the EU's power balance and global security, technological asymmetry, and cooperative measures are also discussed. The evolving military doctrines in the EU, influenced by technological advancements, are explored. The chapter concludes with a forward-looking perspective, offering policy recommendations for responsible innovation, collaborative research, and addressing the challenges inherent in the emerging technologies. Understanding these aspects is crucial to navigate the intricate military technology landscape and ensure a secure future for the European Union.

Andrzej Pawlikowski (2024) 'Emerging and Innovative Military Technologies in the EU Member States: Background and Issues'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 109–158. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_3

Keywords: emerging military technologies, EU Member States, defence capabilities, technological advancements, technological innovation, artificial intelligence (AI), autonomous systems, cyber capabilities, space-based technologies, ethical considerations, legal frameworks, standardisation, proliferation

1. Introduction

Gaining an advantage over the opponent, both on the conventional battlefield, as well as in cyberspace or outer space will depend on capabilities of operational and military technology, including those using the latest technological advancements. Technological progress influences the expansion of military equipment capabilities, and breakthrough technologies. Emerging and disruptive technologies (EDTs)[1] provide potential opportunities to rapidly improve critical parameters and accelerate the process of achieving an advantage over a possible opponent. The use of EDTs in the area of security and defence will have a positive impact on operational capabilities and shape the future battlefield. Hence, the active involvement of European countries in activities aimed at developing and implementing EDTs through national programmes and participation is allied and international partnership initiatives. New ways and means of conducting military operations appear, as well as new, previously unknown, and unidentified threats for which countermeasures must be found. Experience from the conflict in Ukraine is particularly valuable in this context, e.g. in terms of reconnaissance capabilities (acquisition, processing and use of information), command (automated command systems), air defence, and the use of anti-tank means (including the use of unmanned aerial vehicles [UAVs]), as well as the ability to provide logistic support and secure the state's critical infrastructure.

In the rapidly changing international landscape, military technologies are crucial for enhancing countries' defence potential, with European Union (EU) Member States leading the adaptation to new challenges. New technologies, including artificial intelligence (AI), cybersecurity, robotics, and modern communication systems, are pivotal for strengthening defence capabilities and offering innovative solutions for enhancing operational efficiency and effectiveness. This chapter examines the impact of these modern technologies on the defence systems of European countries, examining both the challenges and benefits of their implementation. These technologies not only alter the nature of warfare, but also shape the defence strategies of

1 NATO Advisory Group on Emerging and Disruptive Technologieswas established following a decision by the Heads of State and Government during a meeting in London in December 2019. The group's purpose is to advise NATO on new breakthrough technologies and their strategic implications. Membership is planned for two years, with the potential for a one-year extension. The group includes representatives from Bulgaria, Canada, Denmark, Estonia, France, Spain, Germany, Norway, the U.S., the United Kingdom, and Italy.

states.[2] Understanding the dynamics of these changes is extremely important in the context of the EU, which strives to build a common security and defence policy.[3]

This chapter focuses on the key issues related to emerging military technologies in EU Member States. The technological and political aspects that shape these processes are analysed. Moreover, the author attempts to identify the challenges and benefits related to the adaptation of new technologies in the defence field.

The first part of the chapter provides a brief historical context on the current situation of the EU Member States in the field of military technologies followed by an analysis of the key technologies that constitute the foundation of modern defence capabilities. In the next stage, the political issues involved on the integration of these technologies into the EU's common security and defence policies are discussed.

Finally, the prospects and challenges of emerging military technologies for EU Member States are discussed. This chapter aims to identify important issues and indicate possible directions for development and cooperation in the field of modern military technologies within the EU's defence community.

2. Developing military technologies in the EU

Before examining the latest defense system developments, it is valuable, it is valuable to briefly consider the historical context. Europe, a region marked by centuries of conflict, has continually adapted its defence strategies to evolving political environments and technologies.[4] Traditional defence methods, such as fortification and conventional armies, are evolving into more advanced solutions. The history of defence innovation and technology in Europe has been intertwined with centuries of dynamic military development. European countries have been instrumental in shaping the defence landscape, from medieval fortifications to contemporary cyber systems.[5] The history of European defence technology can be traced back to medieval castles and defensive walls, where innovative systems such as fortresses, defence towers, and underground tunnels were employed to secure strategic areas. In the 19th century, the Industrial Revolution significantly influenced military technology by introducing inventions such as the steam engine, steel, and mass production, leading to the creation of machine guns and artillery. World War I brought a new wave of innovations, including tanks, combat aircraft, and chemical weapons, revolutionising

2 Jonson, 2019, pp. 147–169.

3 The common security and defence policy (CSDP) is an integral part of the EU's common foreign and security policy (CFSP). The role of the European Parliament in the CFSP and the CSDP is defined in Title V, Chapter 2, Section 1 (Common provisions) and Article 36, and the funding arrangements for both policies are set out in Article 41.

4 Bickerton et al., 2022, pp. 173–182.

5 Csernatoni, 2021.

war strategies and emphasising the role of scientific research in the military. During World War II, the development of radar emerged as a key technological achievement.[6] Radar systems have enabled the effective detection of enemy planes and ships, which has been decisive for the course of many battles.[7] During the Cold War, the arms race between the Eastern and Western Blocs spurred innovation in spy satellites, ballistic missiles, and missile defence systems. In response to contemporary threats such as cyberattacks, European nations are prioritising advanced cyber and information security systems to safeguard critical infrastructure. With the increasing digitisation of European societies, cybersecurity has gained prominence in the context of defence. As cyber threats advance, European countries are actively seeking innovative solutions for their detection, response, and prevention. As cyber threats advance, European countries are actively seeking innovative solutions for their detection, response, and prevention.[8]

The ongoing history of defence innovation in Europe reflects a persistent pursuit of security excellence, adapting to scientific progress and geopolitical shifts. In the current global security environment, international cooperation is crucial for effective defence operations. European countries are increasingly collaborating to develop new defence technologies and navigate the challenges associated with such cooperation.

In recent years, the EU has actively engaged in initiatives to develop new military technologies. The landscape of military technology is dynamic, with ongoing and long-term developments. The key aspects related to the EU's involvement in this endeavour are as follows:

- **European Defence Fund**: The EU instituted the European Defence Fund to facilitate collaborative defence research and the development of capabilities among its Member States. The fund promotes cooperation in cutting-edge military technologies, encompassing areas such as AI, cyber capabilities, and advanced materials.[9]
- **Permanent Structured Cooperation (PESCO)**: PESCO provides a framework for EU Member States to strengthen their defence capabilities and collaborate in joint projects. This enables countries to pool resources and share the costs

6 Duignan and Leong, 2023.

7 McMahon, 2021, pp. 76–85.

8 The Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU cybersecurity strategy on 16th December 2020. As a key component of *Shaping Europe's Digital Future*, the *Recovery Plan for Europe* and the *EU Security Union Strategy*, the strategy will bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools.

9 *Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092* (Text with EEA relevance), 2021.

of developing new military technologies across various areas including strategic transport and cyber defence.[10]

- **Defence Innovation Accelerator for the North Atlantic (DIANA)**: DIANA is an organisation established by NATO to find and accelerate dual-use innovation capacity across the Alliance. It provides companies with resources, networks, and guidance to develop deep technologies for solving critical defence and security challenges, from operating in denied environments to tackling threats to our collective resilience.[11]
- **Horizon Europe**: Horizon Europe, the EU's primary research and innovation programme, includes a dedicated pillar for security research that supports advancements in various security-related fields, including defence technologies. The programme promotes collaboration between EU Member States and industry partners to enhance their technological capabilities.[12]
- **Strategic Compass**: The EU is developing a Strategic Compass to guide its common security and defence policy, fostering a shared understanding among Member States regarding common security threats and the capabilities to address them, including the identification and development of emerging military technologies.[13]
- **Cybersecurity and Artificial Intelligence**: Given the increasing importance of cybersecurity and AI in modern defence capabilities, the EU is focusing on these areas. Efforts are underway to develop cybersecurity technologies and strategies as well as guidelines for the responsible development and use of AI in defence.[14]
- **Collaboration with Industry**: The EU underscores collaboration between defence industries and Member States to foster the development of innovative military technologies. Encouraging public-private partnerships is a key approach to leveraging the expertise of both sectors.[15]
- Geopolitical shifts, technological progress, and policy priorities shape the direction and scope of these initiatives. Modern military technologies include AI, autonomous weapons, Big Data, space and quantum technologies, hypersonic missiles, new methods of destruction, drones, stealth technologies, lasers, and electronic weapons. How these innovations impact the combat

10 *Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States*, 2017.

11 Allied Leaders agreed to launch the Defence Innovation Accelerator for the North Atlantic (DIANA) at the 2021 NATO Summit in Brussels, as part of the NATO 2030 agenda, and to establish a multinational venture capital fund to support innovation throughout the Alliance.

12 The Horizon Europe regulation, proposed by the Commission in June 2018, establishes the EU framework programme for research and innovation for the years 2021–2027. It lays down the objectives, the budget, the forms of EU funding and the rules for providing such funding in the field of research and innovation.

13 Document 7371/22, on 24th March 2022, European Union.

14 European Commission, 2021.

15 European Commission, 2022.

capabilities of European armies, and the potential threats associated with their use, are critical considerations.

2.1. Artificial Intelligence

AI has become an integral part of our everyday life, although for many people it is still a concept that is difficult to define. In recent years, AI has revolutionised our lives by reshaping business operations and communication. Beyond robots and autonomous vehicles, AI replicates and enhances human capabilities in learning, analysis, language comprehension, and pattern recognition. Despite some concerns, AI significantly impacts society. This study examines the advantages and risks of AI by examining its seamless integration into daily life. In defence, AI raises ethical and security concerns. Current efforts are focused on AI in cyberspace to analyse and counteract potential attacks. AI combined with VR or AR is poised to enhance military training cost-effectively. Integrating AI into C4ISR systems results in changes, provides secure information for soldiers and commanders, supports threat assessment, and optimises resource utilisation. AI plays a crucial role in electronic warfare by rapidly analysing the electromagnetic environment, facilitating effective countermeasures against attacks, and optimising military radio-frequency management.

Managing the expanding volume of data, particularly with advancing sensor technologies, poses a challenge. Creating a coherent operational picture in multi-domain allied operations, has become increasingly difficult. Advanced command support systems that use AI algorithms will play a crucial role in establishing a Common Operational Picture at higher command levels.

Building trust in artificial intelligence systems requires the use of proven reliable algorithms that operate deliberately and predictably. Another crucial aspect is having extensive databases of reliable and diverse data for AI training. Meeting these requirements is essential for the development of safe and trustworthy systems.

2.2. Autonomy and Autonomisation

Autonomy is an area of breakthrough technology that includes solutions that enable the creation of systems capable of making decisions independently, as well as physical tools to implement these decisions.[16] Considering the complexity of solutions implementing these functions, a more precise formulation is used in the form of autonomous systems (ASs)[17] and when we indicate their connection with physical effectors–robotics and autonomous systems (RAS).[18]

16 Merriam-Webster Dictionary, no date.

17 "Autonomous Systems" mean systems that incorporate artificial intelligence (AI) into the management and control of complex systems. Autonomous systems are operated independently of other management and control systems, though may include human operators (i.e., crew) as part of the operation.

18 Chakraborty, 2021.

Autonomy in decision – making mechanisms and physical tools can mirror the operations and structures of living organisms. This approach, inspired by nature, enables tools to either support or replace humans in the execution of tasks which (i) require maintaining a high level of concentration on the work performed for a long time without the negative effects of fatigue or distraction, (ii) are dangerous to life or health, and (iii) require the development of decisions based on a multi-aspect assessment of the situation using data from multispectral sensor systems and accumulated knowledge resources.

Automation and, in the subsequent stages of development, autonomy of military equipment will take place in various areas, such as reconnaissance, logistics, security, survival of troops, and ultimately, destruction.

Military automation, progressing to autonomy, encompasses reconnaissance, logistics, troop security, and combat. Autonomous reconnaissance platforms excel in information acquisition, conduct missions under diverse conditions, enhance situational awareness, and minimise the risks associated with hidden movements. Autonomous logistics platforms streamline supply delivery in various environments, thereby enhancing subunit mobility and reducing personnel reliance. In troop protection, autonomous recovery platforms swiftly retrieve injured individuals and minimise the exposure of medical personnel to combat. Autonomous combat systems, which have the potential to replace soldiers, are realistically envisioned in human–machine teaching, with human control over crucial decisions. Legal provisions for autonomous combat machines are lacking and pose significant regulatory challenges.

2.3. Analysis, processing and management of large data sets – Big Data

The advantages of the modern battlefield hinges on superior information derived from extensive knowledge of the operational situation and prompt access to essential data. A diverse array of information sources necessitates tools for effective analysis, enabling the identification of relationships and the comparison of anomalies with established patterns in vast datasets. This technological realm is known as Big Data.[19] This concept involves widely distributed databases with synchronisation mechanisms to ensure security, consistency, and data nonrepudiation (e.g. blockchain). It also encompasses robust analytical functions for extracting and presenting the results in the desired accessible format.

As the IoT, advanced reconnaissance, electronic warfare, automated cyber defence, and AI-based command support grow, the analysis of large datasets becomes crucial. Efficient analytical tools in decision-making centres offer a significant advantage on modern battlefields. Cloud and edge computing reduce information exchange latency and installation costs, particularly in hardware, thereby addressing the limitations in data processing for C4ISR systems in tactical environments

19 European Parliament, 2021.

2.4. Quantum technologies

The area of quantum technologies should be considered groundbreaking and can make a significant contribution to the development of defence technologies in the long term. Areas particularly susceptible to the impact of quantum technologies include command support systems at all levels and cybersecurity, communications, and radar technologies.[20]

Quantum computers, with their unique operation, have significantly enhanced computational capabilities compared with conventional machines. Unlike typical PCs, they are tailored for specific tasks, leveraging their efficiency and speed to solve complex mathematical and physical problems. The main challenge in building quantum computers is the accurate extraction of discrete values from the Qbit spectrum[21] states and their instability. Difficulties increase as the number of words for which the calculations are performed increases.

The rise of quantum computers poses a significant threat to existing encryption algorithms, prompting the urgent need for post-quantum safe cryptography solutions. Quantum Key Distribution has emerged as a potential solution for securing key distributions in ICT networks.

Quantum technologies, particularly high-sensitivity sensors and quantum gravimeters, offer significant advancements in submarine navigation. The impact of quantum computing has extended to pattern recognition and analysis, revolutionising reconnaissance techniques in sonar, radio, radar, and satellite technologies. This shift may render the stealth technology less effective for detection.

In defence applications, quantum computers are used to simulate physical and chemical phenomena, aiding in the study of materials for weapons, vehicle armour, aviation, and counteracting CBRN threats. Quantum physics also holds promise for the development of secure communication channels that are resistant to interference and eavesdropping.

Although quantum technologies promise transformative effects on defence capabilities, achieving these outcomes requires long-term and expensive interdisciplinary research. This includes advancements in vacuum, laser, temperature, materials, IT, and electronic circuit manufacturing technologies.

2.5. Space technologies

Drawing on advancements in other fields, space technologies form a distinct research domain because of the unique and often extreme conditions of space and orbital placement. The components of space systems must withstand overloads, shocks, wide temperature variations, and prolonged exposure to cosmic radiation

20 Cornet, Hua and Honggang, 2020, pp. 5–9.

21 "Bit" – a unit of informator in QT, it does not accept discrete values 0 and 1, which are currently used in classical computers.

while maintaining a low electricity demand. Additionally, they require resilience to natural and intentional disruptions, along with effective self-control, monitoring, and removal mechanisms.[22]

Space, which is acknowledged as the fifth operational domain by the Alliance, presents an opportunity to gain an advantage over potential adversaries. Sensors on space platforms, including radar, electro-optical, and thermal sensors, acquire image data that are crucial for reconnaissance to locate and identify enemy activities, infrastructure, and equipment. Earth satellite observation systems and meteorological analyses play vital roles. Precision strikes are essential in armed conflicts, emphasising the importance of developing interference-resistant satellite navigation and time-synchronisation systems.

Satellites supporting global telecommunications maintain crucial communication links during military operations worldwide, thereby contributing to operational awareness. However, dedicated transmission security mechanisms are required for preventing adversary control. Future challenges in space technology applications may involve finding solutions in areas such as quantum technologies for fast and secure communication, Big Data for efficient information searches, AI for satellite platform autonomisation, and advancements in materials and manufacturing technologies.

Satellites may evolve beyond reconnaissance and communication to perform combat missions using kinetic and non-kinetic means, including missile weapons, lasers, and electromagnetic weapons. Countermeasures must be developed to address potential threats to this evolving landscape.

2.6. Hypersonic missile systems

Hypersonic weapons represent the culmination of advanced and expensive technologies, with major military powers approaching their final implementation phase. The global pursuit of supremacy and capacity for pre-emptive strikes, including nuclear strikes, have driven significant financial and technological investments. The primary goal is to establish a deterrent effect that allows one to effectively penetrate enemy air defence by reducing travel times to distant strategic targets. Hypersonic missile systems, primarily within the reach of the world powers, focus on offensive strategic capabilities. Scientific efforts should prioritise measures for detecting, tracking, and neutralising potential threats posed by adversaries using such weapons.[23]

The development and production of hypersonic weapons involve addressing numerous theoretical and technical challenges, including high-performance rocket engines, advanced rocket fuels, hypersonic aerodynamics, engineering heat-resistant materials, guidance theory, motion sensors, automatic pilots, semiconductor electronics, executive mechanisms, radio systems, radio igniters, and warheads. Creating

22 Pahwa, 2023.
23 Seldin, 2022.

an aerodynamic system for a hypersonic rocket body, along with control systems, is a significant interdisciplinary scientific and engineering challenge accompanied by substantial financial commitments, including investment costs for constructing a hypersonic wind tunnel.

2.7. Biotechnologies and technologies to enhance the capabilities of the human body

Biotechnology harnesses living organisms or their components for various functions, such as detecting CBRN threats, influencing organisms, and modifying human bodies to develop or enhance desired features. This may involve operations on human genetic material.[24]

Human Enhancement Technologies aim to improve human abilities in various areas. Strengthening the perception of the environment, also in relation to the tactical situation, is possible by supporting people with devices and interfaces that provide information necessary to perform specific tasks in an easily digestible form. An example of such a solution may be augmented reality systems that supplement the image seen with the naked eye or via a camera with computer-generated objects.[25]

The enhancement of human performance, including physical strength, requires the use of exosuits and exoskeletons. Long-term efforts include biomedical interventions for musculoskeletal augmentation, legal regulations, and moral concerns. The creation of mixed human–machine teams necessitate the development of effective interfaces for controlling such equipment. Human improvement aims to positively increase physiological, cognitive, and social functions by involving various technologies, such as drugs, hormones, implants, and genetic engineering.

2.8. Material and manufacturing technologies

Multidisciplinary research in chemistry, physics, and technical sciences is a source of innovative materials with new or improved properties, the use of which may contribute to the development of military technology and increase the potential of the armed forces. One of the necessary conditions for meeting this challenge is the development of new energy sources and construction materials with high strength and durability.

Advanced construction materials exhibit superior properties such as enhanced mechanical strength, reduced weight, and improved thermal or electrical conductivity. Technologies, such as ceramics, electronic materials, composites, polymers, and biomaterials, have facilitated their production. Intelligent materials capable of intentional property changes combine the sensor, processor, and activator functions. Multifunctional materials, particularly composites, play a vital role in military

24 *Science & Tech*, no date.
25 Pariseau-Legault, Holmes and Murray, 2019.

equipment by providing high strength and stiffness, condition diagnosis, self-repair capabilities, and electromagnetic wave suppression.

Additive technology, including 3D printing, allows the cost-effective and rapid production of monolithic objects and reduces assembly complexity and material usage. This is advantageous in terms of weight reduction and onsite spare-part production for military applications. Joining materials involve various techniques such as welding, lasers, and hybrid methods. Advanced connection methods, such as rivet nuts, are being developed for the efficient design and repair of composite structures using military technology.

Surface modification technologies enhance the hardness, wear resistance, and thermal resistance of construction materials. The application of composite nanolayers to fabrics improves soldier protection and comfort by providing thermal, electromagnetic, and mechanical barriers through optimised coatings.

2.9. Drive systems technologies

Advancements in military technology and the introduction of new types of SPW have necessitated the development of more efficient propulsion, fuel, and power systems with reduced exhaust emissions and alternative operating methods. These developments are closely linked to modern material technologies. Drive systems are becoming increasingly complex and require component miniaturisation, sophisticated measurement devices, and sensors for condition analyses. Modifications to modern engines necessitate the use of appropriate fuels to meet specified standards for both conventional and alternative fuels. These alternative fuels include materials and substances that can replace traditional fuels, nuclear fuels, and artificial radioisotope fuels produced in nuclear reactors.[26]

Advanced fuels offer a pathway to reduce the dependence on conventional hydrocarbon fuels and enhance energy security in European countries and their armed forces. These alternative fuels are expected to possess favourable energy properties, lower the emissions of harmful compounds, and contribute to mitigating the effects of global warming.

2.10. Power sources and energy storage technologies

Currently, most military equipment and components require electricity. To meet the growing demand for electricity and become independent of power sources using fossil fuels, it is necessary to use alternative energy sources and conduct research on their new types.[27]

Converting solar energy into electricity is a priority given the vast potential of solar radiation. Photovoltaic (PV) cells, which are also known as solar cells, are

26 See: ISO, 2021.
27 Wahab, 2014.

crucial for this photovoltaic conversion. Enhancing the efficiency and developing durable structures suitable for military applications, such as foldable mats, are key goals. In military equipment, electronic systems require efficient power sources, and chemical power sources play a vital role in maximising energy accumulation with minimal weight and dimensions to meet the demands of continuous device miniaturisation. The development of new and highly efficient energy storage methods can significantly increase the potential of military technology, which is sometimes used under extreme conditions.[28] They can be used as emergency power sources to maintain the operation of entire systems, helping save energy in vehicles, for example, by allowing the engine to be turned off after stopping and then quickly starting it again. Their use in military equipment may have a positive impact on the start-up of engines at very low ambient temperatures, as well as on the launch of rotating tower mechanisms, other combat systems, and power supply support systems for engineering robots.

2.11. Sensors

Sensors and sensory systems are essential data sources for achieving situational awareness and for supporting operational activities. Reconnaissance tasks rely on imaging devices (optical, multi- and hyperspectral, and laser systems), efficient radars (potentially longer-term quantum radars), and sensors for the electromagnetic environment (analysing the electromagnetic spectrum of the operational space). These devices are applicable to various reconnaissance platforms such as manned, unmanned, autonomous, and military infrastructure facilities. They offer space utilities through satellite equipment and the ground for monitoring potential enemy activities.[29]

Sensory techniques are used in navigation, military protection, survival, and medicine. In navigation, efforts have focused on enhancing the accuracy of positioning and time synchronisation systems across all military platforms, which are crucial for aviation and precision weapons. Quantum gravimeters utilising quantum phenomena are promising for vessels, both surface and underwater, navigating under conditions with limited GNSS signals.

Advancements in destruction systems, including target designation and effective effectors, require sensors for swift threat detection and classification. These, combined with responsive active protection systems, are crucial for increasing the probability of the survival of crew members and supporting equipment on the battlefield.

Sensor technologies for military protection and survival encompass the detection and qualitative assessment of chemical (especially fourth-generation), biological, and

28 *Storage Technology Definitions*, no date.

29 Miklush, no date: 'The sensory system is responsible for detecting and processing sensory information from the environment and converting it into electrical signals that can be interpreted by the brain. The sensory system has two parts: the general sense and the special sense'.

radiological contaminants. These technologies also focus on minimising or altering signatures (magnetic, acoustic, and thermal). Applications range from individual soldier equipment to portable/transportable devices for military units, specialised units, chemical services, and national defence against weapons of mass destruction. Additionally, these sensor technologies detect and identify chemical, biological, and radioactive contamination, adapting to the required level of identification of weapons of Mass Destruction (WMD) factors,[30] various analytical techniques are used. In modern battlefields, the focus is on detecting and identifying WMD agents under field conditions. These include portable contamination detectors, onboard equipment for unmanned aerial vehicles, wearable detectors for individual soldiers, and Wireless Sensor Networks for area monitoring. The development of signature control technologies for land, air, and sea platforms, including unmanned platforms, can reshape future battlefields. Innovations in materials, IT systems, and sensors will enhance the real-time identification, imaging, and control of platform signatures, improving situational awareness, mission effectiveness, and platform survivability.

Medical sensors also play an important role in this context, and biosensors based on biologically active particles demonstrate promise. They measure and evaluate human biological processes, providing insights into a soldier's psychophysical condition, efficiency, and stress levels, which are crucial for determining their ability to perform assigned tasks.

2.12. New destruction systems

Destruction systems alter target characteristics and impacts by employing both kinetic and non-kinetic agents. They provide a versatile spectrum of applications against various threats ranging from temporary disruptions to complete destruction.[31]

Research and development should focus on new means of destruction, including artillery and missile systems, for land, air, sea, and space domains (considering missile systems for space). Improvements should aim to enhance precision and impact force, involving advancements in pyrotechnic materials, initiating devices, and missile propulsion systems. Targeting, identifying, and tracking systems for fast-moving targets are crucial for increased effectiveness.

Directed energy systems such as lasers and electromagnetic weapons are essential for countering emerging threats such as unmanned aerial platforms. In addition, efforts should be made to address systems that disrupt communication and allow the impersonation of an authorised user to take control of the opponent's platform. The development of systems that protect military equipment against enemy influences is critical.

30 UN General Assembly, 1977.
31 Varlamov, Rimshin and Tverskoi, 2018, pp. 808–811.

2.13. Information and telecommunications technologies

The development of information and telecommunications technologies is closely related to the need to achieve an information advantage.[32] The extraction of crucial information relies on analytical tools including Big Data mechanisms and AI algorithms. Ensuring availability at a scheduled time is essential. Although radio signals remain the primary means of data transmission in military tactical systems, cognitive radio and 5G technology offer optimised conditions for cellular communications.

Whether cables, fibre optics, radio, or hybrid communication are used, security is paramount, encompassing confidentiality, non-repudiation, and data integrity. In the cyberspace domain, autonomous cyber response capabilities are crucial for maintaining the availability of command, communication, and weapons support systems, and for ensuring data integrity on the battlefield. Technologically advanced adversaries pose a significant threat to massive cyberattacks targeting military systems and networks. Isolated systems may have limited remote-management capabilities, necessitating autonomous cyber responses and self-configuration abilities.

Developments in quantum technologies have introduced new threats and countermeasures in the information and cyberspace domains. Adapting to global trends in quantum technology is vital for European countries and their armed forces.

2.14. Simulation systems

Simulation systems analyse real objects through digital models, examining the relationships and impacts of decisions on system functioning. Virtual and augmented reality technologies enhance human interaction with digital objects, increase cognitive value, improve effectiveness, reduce costs, and shorten the duration of training projects for the technical maintenance of military equipment.[33]

Efficient algorithms for modelling scenarios and the operational environment are essential for effective military operations management, offering theoretically unlimited possibilities for various actions. An additional benefit is the opportunity for earlier training and preparation of commanders and troops in real operational scenarios.

The idea of digital twins plays a pivotal role in creating new hardware solutions. This study addresses three aspects. First, it provides support for technical analysis (examination of the condition of a real object to improve the planning of service, repair, and maintenance activities). Second, it ensures a digital reflection of the life cycle of a physical object (analysis of its long-term behaviour, prediction of actions/behaviours, ensuring continuity of information at various stages of the life cycle, and management of the life cycle of devices). Third, it supports decision-making by performing engineering and statistical analyses to optimise system behaviour at the design stage, predict development directions, and improve future product performance or parameters.

32 Rouse, no date.
33 Leonelli, 2021, pp. 111–123.

Digital Twin technology enhances the efficient design of new military equipment, expedites production, and minimises previously unknown "childhood" issues. Operational processes benefit from improved efficiency, reducing the downtime caused by equipment failures through optimal scheduling of repairs or technical services. Planning to enhance military equipment can be incorporated into the design stage.

2.15. Medical protection of the battlefield and countermeasures

Medical protection on the battlefield and the organisation of the functioning of the military health service primarily focus on technologies that help overcome challenges related to evacuation and transport, including unmanned transport of injured people and medical supplies, and in conditions of contamination and infection, while maintaining isolation from factors (pathogens) that threaten the health or life of crews and medical staff.[34] In the medical domain, technologies for locating wounded individuals on the battlefield, as well as the automation and robotisation of medical procedures, are of interest. This includes autonomous life and health-support systems. Research on medical protection involves technologies for individual and collective protection against CBRN agents; decontamination of people, animals, and military equipment; and advanced disinfectants for field conditions.

The development of medical countermeasures (MCM), which cover the diagnosis, prevention, and treatment of the consequences of exposure to CBRN agents, is crucial. Improving the technology for diagnosis and treatment remains an ongoing need.

Efficient military health service operations rely on the development of medical information management support systems. These systems track the flow of injured individuals, automate medical documentation processes (e.g. QR coding and chip cards), and utilise AI for diagnostics, decision support, and data analysis. Therefore, research on storage systems for medical supplies and blood products, and additive printing technologies in medicine, including portable 3D printers for medical materials, is necessary.

3. The new selected emerging military technologies in the United States, China and Russia

The U.S. military, comprising the army, navy, and air force, has overcome legacy features through revolutionary innovations in key technological areas. Despite the entrenched sectors, the Defense Advanced Research Projects Agency (DARPA) serves as a unique innovation organisation that addresses military challenges through high-risk, high-reward projects. DARPA's contributions to revolutions in military

34 Saracino, 2019.

affairs, such as precision strikes, stealth aircraft, and unmanned aerial vehicles, highlight its distinct operating characteristics. Officials from the Department of Defense, Congress, and Pentagon are increasingly focusing on developing emerging military technologies to maintain U.S. national security and technological superiority. Initiatives such as the Third Offset Strategy and entities such as the Defense Innovation Unit reflect efforts to exploit emerging technologies for military purposes.

The U.S. Congress and Pentagon officials are intensifying efforts to prioritise cutting-edge military technologies, recognising their critical role in national security. Historically, the U.S. military has relied on technological superiority, but rapid advancements and widespread technology dissemination have posed challenges to established norms. Former Secretary of Defense, Chuck Hagel, highlighted the threat to conventional military advantages. To counteract this, innovation must be fostered by collaborating with the private sector. Initiatives such as innovation hubs and research centres aim to shape the future of U.S. military prowess, ensuring adaptability and proactive influence on global security dynamics.[35] In recent years, the Department of Defense has launched initiatives to counter these technological challenges. The 2014 announcement of the Third Offset Strategy reflects a commitment to leverage emerging technologies for security and military purposes, including strategies, tactics, and operational concepts.[36]

In support of this strategy, the Department of Defense established organisations such as the Defense Innovation Unit and the Defense Wargaming Alignment Group. Aligned with the U.S. National Defense Strategy, these initiatives recognise the impact of rapid technological progress and evolving warfare on national security. This strategy emphasises the importance of cutting-edge technologies such as advanced computing, AI, hypersonic, and biotechnology in shaping future military capabilities. By proactively integrating these advancements, the U.S. aims to stay ahead in the dynamic landscape of modern warfare, address emerging threats, and maintain a strategic advantage in global security.[37] The U.S. leads in technology; however, China and Russia, recognised as strategic competitors, are rapidly advancing sophisticated military technologies. The integration and deployment of these technologies by foreign and domestic military forces have implications for Congressional considerations and global security.

Let us provide an overview of specific emerging military technologies in the United States, China, and Russia: AI, lethal autonomous weapons, hypersonic weapons, directed energy weapons, biotechnology, and quantum technology. This text explores key initiatives within international institutions designed to oversee and regulate the development of emerging technologies. It examines the potential consequences of advancements in military technology and provides an overview of

35 Hagel, 2014.
36 Work, 2014.
37 Department of Defense, 2018.

related concerns for the Congress. These issues may have far-reaching implications for Congressional authorisation, appropriation, oversight, and treaty negotiations.

3.1. Artificial Intelligence[38]

The U.S. government lacks an official definition of ((AI). Policymakers commonly use this term to describe computer systems that exhibit human-level cognition. AI can be categorised into narrow (specific) and general (wide-ranging) tasks. However, true AI systems with human-like cognition currently do not exist, and their realisation is uncertain.[39] Presently, the integration of narrow artificial intelligence is evident in various military applications employed by both the United States and its adversaries. These applications extend beyond intelligence, surveillance, reconnaissance,[40] logistics, cyber operations, command and control, and semi-autonomous and autonomous vehicles. These technologies aim to substitute for and enhance human operators and handle complex tasks. Artificial-intelligence-powered systems can react faster and manage vast data volumes, enabling strategic advantages such as swarming in combat. However, challenges have arisen, including algorithmic biases. Facial recognition programmes exhibit racial bias, emphasising the importance of diverse training data. Gender bias has also been observed in natural language processing programmes, which require careful development and mitigation strategies for AI.[41] Biases in AI used in military settings can lead to unintended harm, especially when lethal consequences are involved. The deployment of AI in lifelike digital forgeries, known as "deepfakes", presents risks, allowing adversaries to exploit this capability for information operations during grey zone conflicts.[42] Deepfake technology poses a threat to the U.S. and its allies, enabling the creation of fake news, the manipulation of public discourse, the erosion of trust, and potential blackmail attempts. Experts suggest that social media platforms should not only deploy detection tools, but also consider broader approaches, such as content authentication, requiring users to specify creation details or label-edited content.

However, some analysts caution against excessive regulation, citing the potential burdens on platforms and concerns regarding free speech. They argued that existing laws and public education efforts are sufficient to address malicious deepfake use.

United States

U.S. non-classified AI investments surged from $600 million in Fiscal Year 2016 to approximately $874 million in Fiscal Year 2022, with over 600 active AI projects

38 See: Sayler, 2020.
39 Bostrom, 2014.
40 Nishawn, 2020.
41 Barrett, 2018; Will, 2016.
42 Theohary, 2023.

overseen by the responsible division. The Department of Defense established a Joint Artificial Intelligence Center in accordance with the 2019 National Defense Authorization Act. This centre, endowed with acquisition authority under Section 808 of the Fiscal Year 2021 National Defense Authorization Act (PL 116-283), supervises AI projects that exceed $15 million.[43] The Joint Artificial Intelligence Center leads National Mission Initiatives in areas such as predictive maintenance, humanitarian aid, disaster relief, war fighter health, and business process transformation. Additionally, it manages the Joint Common Foundation, a secure cloud-based AI development and experimentation environment, for testing and deploying department-wide AI capabilities.[44]

The National Defense Authorisation Act for Fiscal Year 2019 mandates that the Department of Defense create a strategic roadmap for the development and deployment of AI. Guidelines on ethical, legal, and other policies governing the use of AI-enabled systems and technologies in operational scenarios are also required.[45] In support of this mandate, the Defense Innovation Board, an independent federal advisory committee for the Secretary of Defense, has drafted recommendations regarding the ethical use of AI.[46] In line with these suggestions, the Department of Defense embraced five ethical principles for AI, aligned with the recommendations of the Defense Innovation Board: responsibility, equitability, traceability, reliability, and governability. On 26 May 2021 Deputy Secretary of Defense Kathleen Hicks issued a memorandum offering guidance on the implementation of responsible artificial intelligence, in adherence to these ethical principles.[47] The Joint Artificial Intelligence Center is charged with developing and implementing a responsive artificial intelligence strategy, guidance, and policies.[48]

In conclusion, Section 1051 of the Fiscal Year 2019 National Defense Authorization Act established the National Security Commission on Artificial Intelligence. The Commission aimed to assess militarily significant AI technologies and provide recommendations to enhance U.S. competitiveness. The final report, presented to the Congress in March 2021, outlines recommendations across five key lines of effort: investing in development and research, applying AI to national security missions, recruiting and training AI talent, building and protecting United States technological advantages, and marshalling global AI cooperation.[49]

43 Public Law No. 115-232 (2018) Section 2, Division A, Title II, § 1051; and Public Law No. 116-283 (2021) Section 2, Division A, Title VIII, § 808.
44 Available at: https://www.ai.mil/jcf.html (Accessed: 28 February 2024).
45 Public Law No. 115-232 (2019) Section 2, Division A, Title II, § 238.
46 Defense Innovation Board, 2019.
47 Hicks, 2021.
48 Ibid.
49 National Security Commission on Artificial Intelligence, 2021.

China

China is widely recognised as the primary rival of the United States in the global AI market. China's 'Next Generation Artificial Intelligence Development Plan' from 2017 positions AI as a "strategic technology" and designates it as a pivotal focal point in the realm of international competition.[50] China has recently demonstrated significant progress in AI, particularly in language and facial recognition technologies. These advancements are intended for integration into the nation's domestic surveillance network with potential applications in countering espionage and enhancing military targeting capabilities. China is also actively involved in developing autonomous military vehicles for various operations, including swarm technologies, to overcome adversary missile defence interceptors. Open-source information indicates ongoing efforts to create a suite of AI tools for cyber operations.[51] China's oversight of its AI ecosystem contrasts with that of the United States. In China, there are minimal boundaries between the military, the central government, university research laboratories, and commercial enterprises. The National Intelligence Law of China mandates cooperation with the national intelligence, highlighting the interconnected relationships between different sectors and national intelligence efforts. Consequently, the Chinese government has a direct mechanism for steering military AI development priorities and accessing technologies originally developed for civilian applications.

Russia

Russian President Vladimir Putin emphasised that the individual or nation taking the lead in the field of AI will wield a significant influence on a global scale. Currently, Russia lags behind the United States and China in the development of AI. To bridge this gap, Russia has unveiled a national strategy outlining specific benchmarks for the next 5 and 10 years. These goals include enhancing AI expertise, refining educational programmes, expanding datasets, fortifying infrastructure, and refining legal and regulatory frameworks.[52]

Russia affirmed its commitment to persist in implementing its defence modernisation agenda in 2008. The initial plan aimed to incorporate robotics into 30% of the country's military equipment by the year 2025.[53]

The Russian military is actively exploring AI integration, particularly for semi-autonomous and autonomous military vehicles. Recent successes include the development of a combat module for unmanned ground vehicles, which enables autonomous target identification and engagement. Future plans involve expanding

50 China State Council, 2017, p. 2.
51 Kania, 2017, p. 27.
52 See: Office of the President of the Russian Federation, 2019.
53 Simonite, 2017.

autonomous systems with AI capabilities and extending efforts to unmanned aerial, naval, and undersea vehicles, with a specific focus on developing swarming capabilities.[54]

Implementing AI in Russia has the potential to reduce costs and manpower requirements, thereby allowing the deployment of more systems with fewer personnel. Russia is exploring AI applications in remote sensing and electronic warfare to disrupt adversaries' communication and navigation on the battlefield. AI is used extensively in domestic propaganda, surveillance, and information operations. However, achieving substantial progress in AI development may face challenges, as Russian academics rank 22nd globally in AI-related publications[55] and the Russian technology industry has yet to produce AI applications on par with those produced in the United States and China. However, other viewpoints suggest that these factors may be inconsequential. Some analysts argue that historically, Russia has not been at the forefront of Internet technology, yet it has successfully emerged as a significantly disruptive force in the realm of cyberspace.[56] Russia could leverage its expanding technological collaboration with China as a resource.[57]

3.2. Lethal Autonomous Weapon Systems (LAWS)[58]

Lethal autonomous weapon systems (LAWS), as characterised by the Department of Defense Directive, are weapon systems capable of independently identifying and engaging targets without manual human control, often described as "man out of the loop" or „full autonomy". This is distinct from human supervised ("human on the loop") autonomous weapon systems, where operators can monitor and intervene, and semi-autonomous (human in the loop") systems that engage targets selected by a human operator.[59] LAWS rely on computer algorithms and sensor suites to classify objects as hostile, make engagement decisions, and guide weapons to targets. While still in early development, these systems are expected to support military operations in environments with limited communication, thereby addressing operational challenges. Analysts suggest that LAWS can improve the precision in striking military objectives and minimise the risk of collateral damage or civilian casualties.[60]

Approximately 30 countries and 165 non-governmental organisations call for a pre-emptive ban on LAWS due to ethical concerns. Questions about accountability, doubts about adherence to the law of armed conflict's proportionality and distinction requirements, and operational risks are central to advocacy.

54 Bendett, 2017.
55 Konaev et al., 2021, p. 9.
56 Gregory, 2017.
57 Bendett and Kania, 2019, cited in Konaev et al., 2021.
58 See: Lucas, 2016.
59 Department of Defense, 2012.
60 U.S. Government, 2018.

LAWS pose risks, such as hacking vulnerabilities, manipulation of enemy behaviour, unforeseen environmental interactions, and software errors. Unlike automated systems, LAWS lack direct human intervention, increasing the potential for fratricide, civilian casualties, and other unintended consequences.

United States

The United States is not currently developing or deploying LAWS, and none are in its inventory. While there is no explicit prohibition, the Department of Defense Directive offers guidelines for the potential future development and deployment of LAWS, emphasising compliance with the laws of war, treaties, safety regulations, and rules of engagement.[61] This directive includes the requirement that LAWS be designed to „allow commanders and operators to exercise appropriate levels of human judgement over the use of force".[62] Effective decision-making regarding the use of force does not necessitate manual human „control" of the weapon system, contrary to common perception. Instead, it entails extensive human engagement in determining how, when, where, and why weapons will be deployed.

Changes in a system's operational status, particularly those driven by machine learning, demand comprehensive retesting and reassessment of safety and intended functionality. LAWS undergo a dual senior-level evaluation, which includes key figures such as the Under Secretary of Defense for Policy, the Chairman of the Joint Chiefs of Staff, and either the Under Secretary of Defense for Acquisition and Sustainment or the Under Secretary of Defense for Research and Engineering. This evaluation precedes the development and deployment, and a handbook is being developed to guide senior leaders.

China

As noted by Mark Esper, former United States Secretary of Defense, certain Chinese weapons producers, including Ziyan, publicly promoted their weapons by claiming autonomous capabilities in target selection and engagement.[63]

However, the validity of these claims remains unclear. However, it is crucial to note that China lacks explicit prohibitions on the development of LAWS, defining them based on at least five specific attributes:

Lethality entails an ample payload (charge) and the capability to effectively cause harm.

Autonomy refers to the absence of human intervention or control throughout the task execution process.

61 Department of Defense, 2012; Sayler, 2024a.
62 Department of Defense, 2012.
63 See: Tucker, 2019.

The inability to terminate implies that, once initiated, there is no method to halt the device.

The indiscriminate effect implies that the device will execute the task of killing and maiming regardless of the conditions, scenarios, and targets.

Evolution means that, through interaction with the environment, a device can learn autonomously and expand its functions and capabilities in a way that exceeds human expectations.[64]

Russia

Russia has put forth the following definition for LAWS: 'unmanned technical means, distinct from ordnance, designed to execute combat and support missions without operator involvement beyond deciding whether and how to deploy the system'.[65] Russia has recognised that LAWS could improve weapon precision on military targets, potentially reducing unintended strikes on civilians and non-military targets. Although Russia has not explicitly announced the development of such systems, reports suggest that Kalashnikov, a Russian weapons manufacturer, has created a combat module for ground vehicles with autonomous target identification and engagement capabilities.[66]

3.3. Hypersonic Weapons[67]

Several nations such as the United States, Russia, and China are actively advancing the development of hypersonic weapons capable of reaching speeds of at least Mach 5, which is five times the speed of sound. Hypersonic weapons can be broadly classified into two categories: Hypersonic glide vehicles propelled by a rocket upon launch and subsequently gliding towards their target, and hypersonic cruise missiles powered by high-speed engines throughout the flight period.

In contrast to ballistic missiles, hypersonic weapons avoid parabolic ballistic trajectories. They can dynamically manoeuvre toward their targets, making the defence challenging. Analysts differ regarding the strategic implications of hypersonic weapons. Some experts highlight two factors that could significantly influence strategic stability: the brief duration of the weapon's flight, which subsequently compresses the timeline for a response, and the unpredictable trajectory it follows, which could create ambiguity regarding the intended target of the weapon, thereby increasing the likelihood of miscalculation or unintended escalation in the event of a conflict.

64 United Nations, 2018, p. 1.
65 United Nations, 2019.
66 Mizokami, 2020.
67 See: Sayler, 2024b.

However, contrary opinions from some analysts suggest that the strategic impact of hypersonic weapons is limited. They argued that countries such as China and Russia, as competitors to the United States, already have the capacity to target the United States using intercontinental ballistic missiles. These missiles, particularly when launched in salvos, could potentially overpower the U.S. missile defence.[68] Moreover, these analysts contended that the traditional principles of deterrence still apply to hypersonic weapons. They assert, 'It is a significant stretch to envision any regime in the world being so suicidal as to contemplate, let alone execute, the threat or use of hypersonic weapons against the United States… the outcome would undoubtedly be dire'.[69]

United States

In the budget proposal for the Fiscal Year 2022, the Pentagon sought $3.8 billion for the development of hypersonic weapons and an additional $248 million for programmes focused on hypersonic defence.[70] The Department of Defense is actively advancing hypersonic weapons through the navy's conventional prompt-strike programme. This initiative seeks to provide the U.S. military with the capacity to target fortified or time-sensitive objectives using conventional warheads. Progress in hypersonic weapon development is underway through programmes led by the U.S. Air Force, Army, and DARPA.[71]

Analysts supporting these initiatives argue that hypersonic weapons can enhance deterrence and enable the U.S. military to counter threats from mobile missile launchers and advanced air and missile defence systems, which are crucial components of competitors' anti-access/area denial strategies.[72] In contrast, perspectives suggest that hypersonic weapons offer marginal to negligible warfighting advantages. Critics point out that the U.S. military has not yet defined specific mission requirements or operational concepts for these weapons.

The deployment of a functional hypersonic weapon by the United States before 2023 is unlikely. Unlike Russia and China, the U.S. prioritises the development of precision-oriented hypersonic weapons without nuclear warheads, which is a technically challenging endeavour compared with the less accurate Russian and Chinese systems.

China

Experts, including Tong Zhao from the Carnegie Tsinghua Center for Global Policy, believe that China's emphasis on hypersonic technology is driven by the need to counter specific security threats posed by advancing U.S. military technology,

68 Axe, 2019.
69 Raitasalo, 2019.
70 Office of the Under Secretary of Defense, 2021, pp. 2–3; see also Sayler, McCall and Reed, 2020.
71 Freedberg, 2020; Woolf, 2021.
72 Zakheim and Karako, 2019.

particularly the sophistication of regional missile defence. China's pursuit of hypersonic weapons, similar to Russia's endeavours, is driven by concerns that U.S. hypersonic weapons could enable a pre-emptive strike targeting China's nuclear arsenal and support infrastructure. This raises fears that U.S. missile defence systems could limit China's ability to retaliate against the United States. China successfully developed a DF-41 intercontinental ballistic missile capable of carrying a nuclear hypersonic glide vehicle, as reported by the U.S.–China Economic and Security Review Commission in 2014.[73] In February 2020, General Terrence O'Shaughnessy, then-commander of United States Northern Command, confirmed China's testing of a nuclear-capable intercontinental range hypersonic glide vehicle. This vehicle is designed to fly at high speeds and low altitudes, which complicates its ability to provide precise warnings. Indications suggest that in August 2021, China will potentially conduct a test involving a nuclear-capable hypersonic glide vehicle launched by the Long March rocket.[74]

In contrast to China's previous HGV launches using ballistic missiles, Long March employed a Fractional Orbital Bombardment System to launch HGV into orbit. The HGV then deorbits to reach its target, potentially providing China with a space-based global strike capability and reducing the warning time before a strike.[75]

Since 2014, China has conducted at least nine tests on DF–ZF glide vehicle. U.S. defence officials estimate the DF – ZF range to be approximately 1,200 miles, and there are indications that the missile may have the ability to perform evasive manoeuvres during flight.[76] While intelligence agencies have refrained from official confirmation, certain analysts have speculated that DF – ZF may have achieved operational status as early as 2020.[77] In August 2018, China successfully tested Starry Sky-2, a prototype hypersonic vehicle with nuclear capability.[78] Some reports suggest that Starry Sky-2 may become operational as early as 2025.[79] Officials in the United States chose not to provide any comments on the programme.[80]

Russia

Russia began researching hypersonic weapons technology in the 1980s, with an increased focus prompted by the deployment of missile defence systems in the U.S. and Europe. Accelerated efforts followed the United States' withdrawal from the Anti-Ballistic Missile Treaty in 2002.[81] In 2018, Putin voiced concerns over the U.S.

73 U.S.-China Economic and Security Review Commission, 2014, p. 292.
74 Sevastopulo and Hille, 2021.
75 Hadley, 2021.
76 The Economist, 2019.
77 U.S.-China Economic and Security Review Commission, 2015.
78 Yeung, 2018; see also: U.S.-China Economic and Security Review Commission, 2018, p. 220.
79 U.S.-China Economic and Security Review Commission, 2015, p. 20.
80 Gertz, 2018.
81 Borrie, Dowler and Podvig, 2019.

expansion of anti-ballistic missiles, fearing that it could devalue Russia's nuclear capabilities. He warned against the potential interception of all Russian missiles if no action was taken. Russia seeks hypersonic weapons that manoeuvre to penetrate U.S. missile defences, aiming to restore strategic stability.

Russia is actively developing two nuclear-capable hypersonic weapons: the Avangard and 3M22 Tsirkon (or Zircon). The Avangard is a hypersonic glide vehicle launched from an ICBM, granting it an "effectively 'unlimited' range". According to Russian news sources, Avangard became operational in December 2019. Tsirkon, a hypersonic cruise missile designed to be launched from both ships and submarines, has completed previously planned tests in 2021, with series deliveries beginning in 2022.[82]

3.4. Directed Energy (DE) Weapons[83]

According to the Department of Defense, directed energy (DE) weapons use concentrated electromagnetic energy to incapacitate, damage, disable, and destroy enemy targets.[84] DE weapons, with their potential cost advantages and virtually unlimited magazines, can be employed by ground forces for various missions, including short-range air defence (SHORAD), counter unmanned aircraft systems, counter rocket, artillery, and mortar tasks. They offer efficient and effective means of defending against missile salvos and swarms in unmanned systems. Theoretically, DE weapons might also be considered for boost-phase missile intercepts, leveraging their speed of light travel time; however, there are differing opinions on the affordability, technological feasibility, and utility of this application.[85]

High-powered microwave weapons, a subset of DE weapons, can non-kinetically disable electronics, communications systems, and improvised explosive devices. They also have potential as nonlethal "heat ray" systems for crowd control.

United States

Despite the U.S. researching directed energy since the 1960s, experts observe that "real DE programmes" have frequently fallen short of expectations. Despite the Department of Defense investing billions of dollars, many of these programmes have been cancelled.[86] Some researchers argue that advancements in commercial lasers could be used for military purposes.[87] Despite ongoing developments, DE weapons face challenges in terms of technological readiness. Issues include improving beam quality and control to meet military standards, as well as addressing the power,

82 Fediushko and Novichkov, 2021.
83 See: Sayler et al., 2023.
84 Joint Chiefs of Staff, 2020.
85 See: Miller and Rose, 2018.
86 Scharre, 2015, p. 4.
87 See: Ariel, 2015.

cooling, and size requirements for integration into existing platforms. In 2014, the U.S. Navy achieved a milestone by deploying the first operational U.S. DE weapon, the 30-kilowatt Laser Weapon System, aboard the USS Ponce. This prototype demonstrated capabilities such as warnings, blinding enemy forces, shooting down drones, disabling boats, and damaging helicopters.[88] The Navy is currently conducting tests and intends to deploy its 60 kW laser, HELIOS, on the USS Preble in accordance with its deployment schedule. Simultaneously, the army has outlined its plans to introduce its first "combat-relevant" laser, the 50 kW Directed Energy Maneuver-Short Range Air Defense, on Stryker fighting vehicles during Fiscal Year 2022.[89] Similarly, the Air Force is currently engaged in field evaluations of various DE systems designed to counter UAS. These assessments encompass both laser and high-power microwave systems.[90]

In Fiscal Year 2022, the Department of Defense sought a minimum of $578 million for unclassified research, development, test, and evaluation of Directed Energy, and a minimum of $331 million for the procurement of unclassified DE weapons.[91] Several initiatives within these programmes strive to align themselves with the Department of Defense's DE Roadmap. The roadmap charts an increase in DE weapon power levels, targeting approximately 300 kW by the Fiscal Year 2022 and further elevating it to approximately 500 kW by the Fiscal Year 2024.[92]

China

According to the United States – China Economic and Security Review Commission, China initiated the development of DE weapons in the 1980s. The country has demonstrated consistent advancements in the development of High-Power Microwaves (HPM) and progressively more potent high-energy lasers.[93] China has successfully engineered a mobile DE system known as LW-30, boasting a 30-kilowatt capacity. This system is specifically designed to engage unmanned aerial vehicles and precision-guided weapons.[94] Reports suggest that China is developing an airborne

88 Mizokami, 2019, p. 84.

89 See: Seapower Staff, 2021; Office of the Under Secretary of Defense, 2021.

90 See: Mizokami, 2020.

91 These figures include funding for DOD wide programmes as well as programmes managed by the Air Force, Army, and Navy. CRS analysis of FY2022 budget documents; for additional information, see: Appendix B in Sayler et al., 2023, pp. 228–256.

92 Although there is no consensus regarding the precise power level that would be needed to neutralize different target sets, it is generally believed that a laser of around 100 kW could engage UAVs, small boats, rockets, artillery, and mortar, whereas a laser of around 300 kW could additionally engage cruise missiles flying in certain profiles (i.e., flying across rather than at the laser). Dr. Jim Trebes, „Advancing High Energy Laser Weapon Capabilities: What is OUSD (R&E) Doing?" Presentation at IDGA, October 21, 2020; and CRS conversation with Principal Director for Directed Energy Modernization Dr. Jim Trebes, November 17, 2020. Required power levels could be affected by additional factors such as adversary countermeasures and atmospheric conditions and effects.

93 See: U.S.-China Economic and Security Review Commission, 2017, p. 563.

94 See: Novichkov, 2018.

energy weapons pod. China has used or proposed DE weapons from the United States and its allies to interfere with military aircraft. Additionally, these weapons have been considered to disrupt the U.S. freedom of navigation operations in the Indo – Pacific region.[95]

According to the Defense Intelligence Agency, China is actively exploring DE weapons to disrupt satellites and sensors. These signs indicate China's limited capability to use laser systems for satellite sensors. The deployment of ground-based laser weapons to counter low-orbit space-based sensors is expected, with potential higher-power systems posing a threat to the structural integrity of non-optical satellites.[96]

Russia

Since the 1960s, Russia has actively pursued DE weapons research, with a specific emphasis on HELs. Reports suggest that Russia has operationalised Peresvet, a mobile ground – based HEL deployed alongside mobile intercontinental ballistic missile units. Although details about Peresvet, including its power level, are mostly unknown, some analysts speculate on its potential use for satellite dazzling and as a point defence system against unmanned aircraft systems.[97] The Deputy Defence Minister of Russia, Alexei Krivoruchko, has announced ongoing efforts to enhance the power level of the Peresvet, and intends to deploy it on military aircraft.[98]

Reports suggest that Russia is exploring HPMs and developing additional high-energy lasers capable of conducting anti-satellite missions.

3.5. Biotechnology

Biotechnology, drawing from life sciences, propels technological advancements with substantial implications for the U.S. military and global security. In 2018, a report from the Government Accountability Office highlighted the recognition of the potential impact of biotechnologies by key entities, including the Departments of Defense, State, and Homeland Security, as well as the Office of the Director of National Intelligence. Notably, low-cost gene editing tools, such as CRISPR, are at the forefront of technologies garnering attention in this context and[99] have the potential to alter genes or create DNA to modify plants, animals, and humans. Biotechnology has the potential to enhance military personnel's capabilities. The widespread adoption of synthetic biology, which allows for the creation of genetic codes that

95 See: Tate, 2020; Patrick and Ryan, 2020.
96 Defense Intelligence Agency, 2019, p. 20.
97 Defense Intelligence Agency, 2019, p. 23.
98 See: Hendrickx, 2020.
99 See: Gallo et al., 2018.

are not found in nature, may increase the number of entities capable of developing chemical and biological weapons.[100]

Similarly, the 2016 Worldwide Threat Assessment by the United States Intelligence Community identified genome editing as a possible tool for mass destruction. Moreover, biotechnology has the potential to create adaptive camouflage, cloaking devices, advanced, lighter, stronger, and potentially more self-healing bodies, and vehicle armour. Concerns have arisen about the ethical standards followed by U.S. competitors in the research and application of biotechnology, especially in the realms of biological weapons, genome editing, and more intrusive forms of human performance modification.

United States

In accordance with Section 1086 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328),[101] the Donald Trump Administration released the National Biodefense Strategy, which outlines 'how the United States Government will manage its activities more effectively to assess, prevent, detect, prepare for, respond to, and recover from biological threats, coordinating its biodefence efforts with those of international partners, industry, academia, non-governmental entities, and the private sector'. However, analysts note that this strategy lacks a well-supported action plan and remains largely unimplemented. However, the Department of Defense lacks specific biotechnological research strategies. Unclassified U.S. biotechnology programmes for military applications have primarily focused on enhancing readiness, resilience, and recovery. DARPA has initiated various biotechnology programmes addressing battlefield medicine, diagnostics, prognostics, traumatic brain injuries, neuropsychiatric conditions, infectious diseases, and bioengineered threats to the U.S. food supply. DARPA's Safe Genes programme aims to protect service members from unintended or deliberate misuse of genome editing technologies.

Service laboratories have concluded a $45 million three-year joint research initiative in synthetic biology, focusing on innovative bio-based materials and sensors. The United States is exploring biotechnology and neuroscience applications to enhance soldier lethality, aiming for stronger, smarter, and more capable soldiers; however, there is no national framework for ethical considerations.

The Department of Defense, in response to Section 278 of the Fiscal Year 2021 National Defense Authorization Act, conducts a comprehensive evaluation of the military implications of emerging biotechnologies. This aims to provide insights and recommendations for potential legislative and administrative actions in the future. As mandated in Section 278, the Department of Defense assesses emerging

100 Government Accountability Office, 2018, p. 28.
101 Public Law No. 114-328 (2016) Section 2, Division A, Title X, § 1086.

biotechnologies for national security purposes, involving a direct comparison of the capabilities of the United States and other countries.[102]

China

Owing to the challenges of an ageing population and rising healthcare demands, China is actively advancing biotechnological research. Recognised as a crucial strategic priority under the Made in China 2025 initiative and emphasised in the ongoing five-year development plan, biotechnology reflects China's commitment to addressing healthcare and demographic concerns.[103] China is actively advancing biotechnology, particularly in genetic testing and precision medicine. In 2016, Chinese scientists achieved a milestone by using the CRISPR gene editing tool in humans. In 2018, a Chinese scientist, possibly with government approval, generated the first "gene edited babies". China houses National GenBank, one of the world's largest genetic information repositories, which includes data from the United States. These data can be used for personalised disease treatment or precise bioweapons. Although detailed information on China's military biotechnology applications is limited, the military civil fusion policy allows for the easy integration of civilian advancements for military purposes, highlighting the dual-use nature of biotechnological developments in China.

Reports indicate that China's Central Military Commission has allocated funding for projects in military brain science, advanced biomimetic systems, biological materials, human performance enhancement, and innovative biotechnology. Chinese military medical institutions are actively involved in CRISPR gene editing research. These initiatives highlight China's strategic interest and investment in advanced technologies with applications in both military and medical contexts.

Russia

Despite the release of BIO2020, a comprehensive government strategy aimed at enhancing Russia's biotechnology sector in 2012, biotechnology research in Russia still lags behind that in the United States and China.[104] BIO2020 outlines Russia's biotechnological research focus, which spans biopharmaceutics, biomedicine, industrial biotechnology, bioenergetics, agriculture, food biotechnology, forest biotechnology, environmental protection biotechnology, and marine biotechnology. Limited public information exists on how Russia may apply these dual-use technologies in the military or national security contexts. Concerns have arisen owing to attempts to assassinate a former double agent using a Novichok nerve agent, raising the possibility of exploiting biotechnological advancements for weaponising biological agents,

102 Public Law No. 116-283 (2021) Section 2, Division A, Title II, § 278.
103 See: CSET, 2021.
104 Russian Federation, no date.

including synthetic biology. The Soviet Union's history of maintaining a secretive biological weapons programme, Biopreparat, in violation of the 1972 Biological Weapons Convention adds to these concerns.

In August 2020, the End User Review Committee, comprising representatives from U.S. Departments of Commerce, State, Defense, Energy, and, when applicable, Treasury, found "reasonable cause" to suspect three Russian research institutes are linked to the Russian biological weapons programme.[105]

3.6. Quantum Technology

Quantum technology applies principles from quantum physics to practical applications, with significant potential implications for military sensing, encryption, and communications. Although not yet mature, reports from the Government Accountability Office indicate collective assessments by the Departments of Defense, State, Homeland Security, and the Office of the Director of National Intelligence. They suggest that „quantum communications could empower adversaries to establish secure communications beyond the reach of interception or decryption by United States personnel". Quantum computing poses the risk of potentially enabling adversaries to decrypt sensitive information and exposing U.S. personnel and military operations to targeted threats. Additionally, quantum technology could have military applications, such as quantum sensing, enhancing submarine detection and effectively making the oceans „transparent". Quantum sensing poses a potential threat to the resilience of U.S. sea-based nuclear deterrents, while also offering alternatives for positioning, navigation, and timing in GPS-degraded or denied environments. However, the application of quantum technologies in military contexts is challenging owing to the delicate nature of quantum states, which can be disrupted by slight movements, temperature variations, or other environmental factors. Physicist Mikkel Hueck noted that if quantum devices require extremely low temperatures, they can be costly, cumbersome, and energy-intensive. Achieving widespread adoption depends on notable advancements in materials science and fabrication techniques.

United States

According to an assessment by the Defense Science Board Task Force on Applications of Quantum Technologies, the U.S. military stands to benefit significantly from three key applications of quantum technology: quantum sensing, quantum computing, and quantum communications. The task force underscored the potential of QS to significantly enhance the capabilities of the Department of Defense for specific missions, providing precise navigation and timing in GPS-compromised environments. It also recognises the potential of quantum computers for decryption, signal processing, and AI applications, along with the enhancement of networking

105 Department of Commerce, 2020.

technologies through quantum communications. The assessment concluded that quantum sensing is ready for mission deployment, whereas quantum computing and communications are still developing early. The idea that quantum radar enhances the capabilities of the Department of Defense has been dismissed. DARPA and various military services allocate funding to diverse quantum technology programmes coordinated under Section 234 of the Fiscal Year 2019 NDAA to facilitate interagency collaboration in quantum information science and technology research and development.[106]

Under Section 220 of the Fiscal Year 2020 NDAA, each military department's secretary is authorised to establish quantum information science research centres. These centres can engage with public and private sector organisations to advance research in the field of quantum information science.[107] To date, the Navy has designated the Naval Research Laboratory as its Quantum Information Science Research Center, whereas the Air Force has chosen the Air Force Research Laboratory to serve both the Air and Space Forces. However, the army has stated that it currently has no plans to establish a quantum information science research centre.

As per Section 214 of the Fiscal Year 2021 NDAA, services must regularly update their list of technical challenges that quantum computers can address in the next one to three years. This section also mandates collaboration with small- and medium-sized businesses to provide quantum computing capabilities to the government, industry, and academic researchers addressing these challenges. In a related directive, Section 1722 mandates that the Department of Defense should assess the risks posed by quantum computers and evaluate the existing standards for post-quantum cryptography.

China

China has placed growing emphasis on advancing quantum technology research as a key focus within its broader developmental strategies.[108]

President Xi prioritised quantum communications and computing for major breakthroughs by 2030, aligning with China's National Science and Technology Innovation Program. In 2016, a quantum technology leader in China deployed the first quantum satellite for global quantum encrypted communications. In 2017, China solidified its leadership by hosting its first quantum-secured intercontinental videoconference.[109] China has invested heavily in terrestrial quantum communication networks. In 2016, a 2,000 kilometre quantum network linking Beijing and Shanghai was established. Ambitious plans are in place to expand the nationwide network in

106 Public Law No. 115-232 (2019) Section 2, Division A, Title II, § 234.
107 Public Law No. 116-92 (2019) Section 2, Division A, Title II, § 220.
108 Kania and Costello, 2018.
109 Office of the Secretary of Defense, 2019, p. 101.

coming years.[110] While quantum technology has developed primarily through academia, China aims to leverage these advancements for military applications, as outlined in its Thirteenth Five-Year S&T Military Civil Fusion Special Project Plan.

Russia

Russia's progress in quantum technology, similar to its advancements in AI, is significantly behind those of the United States and China. Analysts observe that Russia is potentially „5 to 10 years behind" particularly in the realm of quantum computing.[111] To expedite advancements, Russia announced in December 2019 a $790 million in quantum research over the next five years. The country has also adopted a five-year Russian quantum-technology roadmap to provide direction and structure for its quantum-technology development.[112] Although not exclusively focused on the military, details on how Russia plans to integrate these initiatives into its military operations are sparse in open sources.

4. Potential implications of Emerging Technologies for Warfighting

The rapid and relentless advancement of technology is a transformative force that has undeniably altered the warfare landscape. This profound influence not only redefined the methods by which nations engage in conflict but also prompted a paradigm shifts in the formulation and execution of defence strategies. Among the array of groundbreaking technologies at the forefront of this evolution are AI, autonomous systems, cyber capabilities, and biotechnology. These emergent technologies possess the unprecedented potential to revolutionise the very essence of warfighting, from the tactical intricacies of military operations to the broader realms of strategic thinking and ethical considerations.

AI, the cornerstone of this technological revolution, introduces a spectrum of possibilities that extend far beyond traditional military applications. The integration of AI into defence systems holds promise for enhancing decision-making processes, augmenting the efficiency of resource allocation, and optimising overall operational effectiveness. By leveraging advanced algorithms capable of processing vast volumes of data, military commanders can obtain real-time insights, enabling more informed and adaptive responses on the battlefield. However, this infusion of AI into military affairs is not without challenges, as it brings to the forefront concerns about

110 Kania and Costello, 2018.
111 See: Quirin, 2019.
112 Public Law No. 115-368, 2018.

algorithmic biases, the potential for unintended consequences, and ethical considerations surrounding the deployment of lethal autonomous weapons.

Similarly, autonomous systems encompassing unmanned aerial vehicles (UAVs), ground vehicles, and naval drones represent revolutionary forces reshaping the dynamics of warfare. The ability of these systems to perform an array of tasks without direct human intervention (from reconnaissance missions to targeted strikes) holds promise for reducing human casualties, while enhancing operational capabilities. However, the advent of autonomy in military systems has created profound ethical dilemmas. Delegating lethal decision-making to machines poses questions about accountability, unintended collateral damage, and the establishment of robust ethical frameworks that govern their use in compliance with international norms.

Cyber capabilities have emerged as a critical dimension of modern warfare as nations increasingly harness the power of digital domains to gain strategic advantages. The ability to conduct sophisticated cyberattacks on an adversary's infrastructure, disrupt communication networks, and compromise sensitive information has become a defining feature of contemporary conflicts. However, the inherently interconnected nature of cyberspace exposes vulnerabilities that extend beyond the traditional geopolitical boundaries. It is imperative to strike a delicate balance between offensive cyber operations and the need for resilient cybersecurity measures, underscoring the importance of establishing international norms that govern this evolving domain.

Biotechnology, with its revolutionary strides in genetic engineering and human augmentation, has introduced a new frontier in warfighting capabilities. The potential to enhance physical and cognitive abilities, coupled with personalised medical treatments, could redefine the capabilities of individual war fighters. However, the ethical considerations surrounding the creation of super soldiers, potential violations of human rights, and the geopolitical implications of imbalances in biotechnological advancements require careful scrutiny. Striking a balance between technological innovation and ethical boundaries is imperative to ensure responsible development and deployment of biotechnological advancements.

As space becomes an increasingly contested domain, its militarisation introduces novel challenges and opportunities for warfare. Nations have viewed space dominance by investing in satellite technologies for communication, surveillance, and navigation. The potential for satellite-based attacks introduces a new dimension to conflicts, raising concerns about the weaponisation of space and the need for international cooperation to prevent destabilising space-based confrontations.

Quantum technologies, which encompass quantum computing and communication, present a disruptive force that challenges existing paradigms of cryptography and secure communication. The development of quantum capabilities provides strategic advantages; however, the potential obsolescence of existing encryption methods raises concerns about the vulnerability of military communications. Adapting to the quantum era requires technological innovation as well as the establishment of new cybersecurity measures and international cooperation to address the asymmetric threats posed by quantum technologies.

Given these technological advancements, ethical and legal considerations are on the horizon. The integration of AI, autonomous systems, biotechnology, and other emerging technologies into warfighting requires the formulation of ethical guidelines and legal frameworks governing their use. Questions about the responsible use of AI, autonomy of lethal systems, and potential consequences of biotechnological enhancements require global collaboration to establish norms that prevent misuse and ensure accountability.

The introduction of emerging technologies also necessitates a fundamental re-evaluation of military doctrines and strategies. Nations must adapt to the changing landscape by integrating these technologies into existing frameworks while developing novel operational concepts. Harnessing the advantages of emerging technologies while mitigating their risks is essential for maintaining strategic relevance and ensuring preparedness on modern battlefields.

The multifaceted implications of emerging technologies for warfighting extend across various dimensions from the intricacies of military operations to the broader realms of strategic thinking and ethical considerations. As nations navigate this era of unprecedented technological progress, international cooperation has become paramount for establishing norms, regulations, and ethical guidelines that ensure responsible and accountable use. Striking a delicate balance between innovation and ethical considerations is imperative to navigate the evolving landscape of modern warfare and promote stability in an era characterised by rapid technological advancements.

4.1. Artificial Intelligence and Machine Learning

AI and machine-learning technologies offer unprecedented opportunities and challenges in warfare. These systems can enhance decision-making processes, optimise resource allocation, and improve overall operational efficiency. AI-driven algorithms can analyse vast amounts of data and provide commanders with real-time insights for strategic planning. However, reliance on AI also introduces vulnerabilities such as the risk of algorithmic biases, hacking, and ethical concerns regarding the use of lethal autonomous weapons.

4.2. Autonomous Systems

The development of UAVs, autonomous ground vehicles, and naval drones has reshaped battlefields. These systems can perform various tasks ranging from reconnaissance to targeted strikes without direct human control. While autonomous systems can reduce human casualties and enhance operational capabilities, there are ethical dilemmas surrounding the delegation of lethal decision-making to machines. The potential for unintended consequences and need for robust ethical frameworks pose challenges for policymakers and military leaders.

4.3. Cyber Warfare

The digital realm has become critical in modern warfare. Cyber capabilities enable nations to conduct sophisticated attacks on adversary infrastructures, disrupt communication networks, and compromise sensitive information. Offensive cyber operations can be conducted covertly, thus providing strategic advantages. However, the interconnected nature of cyberspace exposes vulnerabilities to potential retaliation and escalation. Establishing international norms and rules for cyber warfare is essential for mitigating the risks associated with this emerging domain.

4.4. Biotechnology and Human Augmentation

Advances in biotechnology, including genetic engineering and human augmentation, can redefine war fighter capabilities. Enhanced physical and cognitive abilities as well as personalised medical treatment could provide a significant advantage on the battlefield. However, ethical concerns have arisen regarding the potential to create super soldiers, violate the principles of human rights, and exacerbate existing geopolitical tensions. Balancing innovation with ethical considerations is crucial for the development and deployment of biotechnological advancements.

4.5. Space Dominance

Space has become a contested domain with nations investing in space-based technologies for communication, surveillance, and navigation. The militarisation of space introduces the potential for satellite-based attacks, which disrupt adversary capabilities and communication networks. As nations compete for space dominance, there is a growing need for international cooperation and the establishment of norms to prevent the weaponisation of space and mitigate the risks of space-based conflicts.

4.6. Quantum Technologies

The development of quantum computing and communication has implications for cryptography, intelligence gathering, and secure communication. Quantum technologies can potentially render existing encryption methods obsolete, posing challenges to securing military communication. Nations investing in quantum capabilities gain a strategic advantage; however, this also raises concerns regarding the potential for asymmetric threats and the need to adapt cybersecurity measures in the quantum era.

4.7. Ethical and Legal Considerations

The integration of emerging technologies into warfighting necessitates the careful consideration of ethical and legal frameworks. Questions surrounding the responsible use of AI, autonomy of lethal systems, and potential consequences of biotechnological

enhancements require international collaboration to establish ethical guidelines. Developing legal norms governing the use of emerging technologies in armed conflicts is crucial for preventing misuse and ensuring accountability.

4.8. Adaptation of Military Doctrine

The introduction of emerging technologies requires a fundamental shift in military doctrine and strategy. Nations must adapt to the changing landscape by integrating these technologies into existing frameworks while developing new operational concepts. Harnessing the advantages of emerging technologies while mitigating their risks is essential for maintaining strategic relevance on modern battlefields.

The dynamic landscape of modern warfare has been increasingly shaped by the rapid evolution of emerging technologies, presenting a myriad of potential implications across various domains. At the strategic level, nations are compelled to reconsider traditional doctrines and strategies to effectively integrate cutting-edge technologies into their defence capabilities… Operational implications extend to the battlefield, where advancements in AI, autonomous systems, and cyber capabilities are transforming the nature of conflict and military operations.

Ethical considerations are significant in this era of technological progress, as the deployment of advanced weaponry and surveillance systems raises concerns about the potential for unintended consequences and civilian casualties. Striking the right balance between innovation and ethical considerations is essential for ensuring that the development and application of emerging technologies align with international humanitarian laws and ethical norms. For instance, the ethical dimensions of autonomous weapons require careful scrutiny to prevent loss of human control and mitigate the risk of unintended consequences.

On the legal front, there is a pressing need for the international community to collaborate and establish clear regulations governing the use of emerging technologies in warfare. International law must adapt to address the challenges posed by novel weapons systems, cyber warfare, and other technologically driven aspects of conflict. This requires a proactive approach to developing and updating legal frameworks that can effectively govern the responsible use of emerging technologies while holding violators accountable.

Collaboration among nations is paramount in addressing the potential consequences of emerging warfare technologies. The establishment of international norms and agreements will contribute to a more stable and secure global environment. A shared commitment to ethical guidelines can serve as a foundation for responsible behaviour, preventing the misuse of advanced technologies that could escalate conflicts and endanger global security.

As nations continue to invest heavily in the development of emerging technologies for warfighting, it is crucial for the international community to foster collaboration and establish comprehensive norms, regulations, and ethical guidelines. Striking a balance between innovation and ethical considerations is imperative for

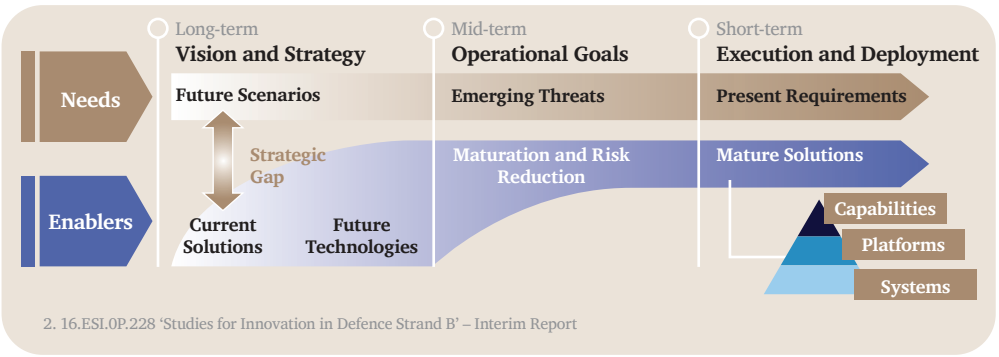
navigating the complexities of modern warfare and ensuring a stable and secure global landscape in the face of rapid technological advances

5. Defence innovation: future perspective

Rapid technological changes, including defence, have shaped the pace of life in society. The level of protection a state offers its citizens depends on its ability to defend itself against technological interference. Strategic and technological forecasting is crucial for the European Armed Forces to invest in their future capabilities. The concept of innovation is widely used across various fields, but there is ambiguity about what qualifies as „innovative". Over time, innovation shifted from having a negative connotation to becoming a key factor in long-term economic growth and international competitiveness.

Innovation involves creating and applying new products, services, and processes, including adapting existing technologies to different challenges. Integrating diverse innovative technologies into defence can reduce the initial investment risks and the time to deliver new military capabilities. The objective is not only to conceive novel concepts, but also to provide added value to end users, with a focus on enhancing military capabilities. Innovation in the defence sector can take various forms. Breakthrough innovations significantly affect operational methods and market dynamics, leveraging enabling factors to surpass traditional progress. By contrast, gradual innovations aim to optimise existing products, services, or processes without fundamentally altering them.

Table 1 – Future scenarios determined at the stage of long, mid, and short vision and strategy[113]



113 European Defence Agency, 2017, p. 9.

Successful defence sector innovations require a blend of breakthroughs and gradual innovation capabilities to meet future defence requirements. Organic innovation occurs in response to new threats and gaps in strategic capabilities. Long-term vision and strategies are vital for anticipating challenges and allocating resources to emerging technologies. Although structured processes are essential to innovation, they must be streamlined to encourage creativity. Unlike traditional defence-led models, recent trends have shown that civil and commercial markets drive innovation in fundamental technologies. The European Defence Agency prioritises collaboration with nontraditional research communities to efficiently access groundbreaking research. The Captech Technology Group within the agency plays a key role by establishing a network of experts from the participating Member States to address specific technology areas.

The European Defence Agency has implemented a comprehensive tool chain to enhance innovation and integrate new subjects and technologies into defence. This tool chain covers all stages, from identifying technology and project concepts to enhancing the overarching strategic research programme, known as the Overarching Strategic Research Agenda.[114]

1. The "Technology Watch" initiative is a recent undertaking launched by the European Defence Agency. Its aim is to empower research and technology experts to actively seek and disseminate new information among their peers. Furthermore, a dedicated technological forecasting methodology is devised to facilitate the long-term identification of emerging technologies.
2. Captechs identify the technologies discussed in the Technology Watch tool and forecasting workshops. In the second stage, the collective expertise of all the participating member states is harnessed for technological assessment. This involves determining the best practices and implementing customised processes intended to evaluate interest in a specific technology.
3. The final stage involves selecting the most promising technologies to incorporate into an Overarching Strategic Research Agenda.

The analysis of the above time horizons to achieve maturity has been categorised into five different perspectives, each with a specific timeframe:

1. Short-term perspective: This indicates that maturity is achieved within the next five years. This is the most immediate timeframe, suggesting a relatively quick realisation of goals or completion.
2. Short- and medium-term perspectives: This timeframe suggests that maturity will be achieved between 5 and 10 years. It covers both the short-term and beginning of the medium-term range, indicating a moderate waiting period.
3. Short- and medium-term perspectives: This timeframe suggests that maturity will be achieved between 5 and 10 years. It covers both the short-term and beginning of the medium-term range, indicating a moderate waiting period.

114 *Disruptive Defence Innovations Ahead!*, no date.

4. Short- and medium-term perspectives: This timeframe suggests that maturity will be achieved between 5 and 10 years. It covers both the short-term and beginning of the medium-term range, indicating a moderate waiting period.
5. Short- and medium-term perspectives: This timeframe suggests that maturity will be achieved between 5 and 10 years. It covers both the short-term and beginning of the medium-term range, indicating a moderate waiting period.

Each perspective helps plan and set expectations based on the anticipated timeframe for maturity. This compilation is derived from an analysis of long-term technological trends outlined in the ability development plan, along with groundbreaking technologies identified by Captech at the European Defence Agency during the Overarching Strategic Research Agenda process.[115]

6. Conclusions and recommendations

In scrutinising the dynamic landscape of emerging military technologies across EU Member States, it becomes increasingly apparent that the region stands at a pivotal crossroads. Innovation, security imperatives, and ethical considerations converge, creating a complex matrix that requires a nuanced analysis. The interplay of cutting-edge technologies, geopolitical dynamics, and ethical frameworks presents a multifaceted puzzle that necessitates a comprehensive examination to comprehend fully.

Our journey highlights the latest achievements, shedding light on the strides made in various technological domains that contribute to the defence apparatus. Simultaneously, we confront the challenges that have arisen in this era of rapid technological evolution and address concerns related to cybersecurity, geopolitical tensions, and the ethical dimensions of deploying advanced military capabilities.

Moreover, our scrutiny extends beyond the present moment, with the aim of forecasting development prospects. By doing so, we seek to anticipate the trajectory of European defence systems in the face of evolving global dynamics, thereby providing insights into the strategic considerations that will shape the region's security landscape.

Ultimately, the overarching objective is to understand how these new technologies are not only reshaping the face of European defence, but also to discern the far-reaching implications they hold for the broader spectrum of regional security. By navigating the intricate web of innovation, security imperatives, and ethical frameworks, we aspire to contribute to a comprehensive understanding of the intricate

115 See: European Defence Agency, 2019.

tapestry that defines the contemporary landscape of European defence in the age of advanced technologies.

This exploration unearthed several key insights and issues that demand attention from policymakers, defence experts, and the broader public. Several noteworthy findings emerged from this examination.

1. **Technological Leapfrogging and Competitiveness.**
   EU Member States are actively engaging in a technological arms race driven by the imperative to maintain military competitiveness in an era characterised by rapid advancements. The pursuit of cutting-edge capabilities reflects a strategic commitment not only to keep pace with global developments but also to potentially lead in certain areas. Member States must strike a delicate balance between cooperation and competition to foster an environment that promotes innovation without compromising security.
2. **Collaboration Challenges and Opportunities.**
   A collaborative landscape presents both challenges and opportunities. While the European Defence Fund and other initiatives aim to foster cooperation, Member States must navigate political, economic, and technological divergence. Overcoming these challenges demands a shared vision, standardised protocols, and commitment to the common security interests of the EU. Enhanced collaboration has the potential to streamline research efforts, optimise resource allocation, and amplify the impact of emerging military technologies.
3. **Ethical and Legal Implications.**
   The deployment of emerging military technologies has raised profound ethical and legal questions. As autonomous systems, AI, and cyber capabilities become integral to defence strategies, there is an urgent need for a robust ethical framework. Establishing clear guidelines for the ethical use of military technologies is not only a moral imperative, but also essential for maintaining public trust and adherence to international norms. Striking the correct balance between innovation and responsible use requires a multidisciplinary approach involving policymakers, ethicists, and technologists.
4. **Strategic Autonomy and Global Partnerships.**
   The quest for strategic autonomy is a defining feature of the EU's approach to emerging military technologies. However, this should not be viewed as an isolation. A nuanced strategy involves the careful calibration of autonomy and the forging of global partnerships. Recognising the interconnected nature of security challenges, the EU must leverage its technological strength to contribute to international stability. Collaborative ventures with like-minded nations and organisations can enhance the effectiveness of security efforts while mitigating the potential risks associated with unilateralism.
5. **Resilience and Adaptability in the Face of Uncertainty.**
   The dynamic nature of technological advancement introduces uncertainty. Member States must cultivate resilience and adaptability in their military

strategies. Thus, a flexible approach that accommodates rapid technological changes is crucial. Investing in versatile capabilities, fostering a culture of continuous learning, and prioritising agility in decision-making are essential components of a resilient defence posture.

6. **Public Engagement and Transparency.**
The implications of emerging military technologies extend beyond defence establishments to impact society. Public engagement is paramount for shaping policies that align with societal values and concerns. Transparency in the development and deployment of military technologies fosters public trust and ensures democratic supervision. Member States should actively communicate their strategies, risk assessments, and ethical considerations to build a shared understanding of the role of technology in national and collective security.

In conclusion, the trajectory of emerging military technologies within the EU Member States has significant implications for a region's security landscape. Successful navigation of this complex path demands a nuanced approach that strikes a delicate balance between competition and collaboration, autonomy and global partnerships, and innovation and ethical considerations. The decisions of EU Member States to steer this trajectory will undoubtedly shape the future dynamics of security and defence in the region.

Maintaining a competitive edge while fostering collaboration among Member Statesis crucial for bolstering the EU's collective defence capabilities. The pursuit of technological advancements should be accompanied by a commitment to work together to address common security challenges. By fostering a cooperative environment, Member States can pool resources, share expertise, and enhance interoperability, thereby creating more robust and unified defence postures.

Simultaneously, the pursuit of autonomy in military technologies should be tempered by recognising the interconnected nature of global security. Striking a balance between autonomy and strategic partnerships with like-minded nations is essential for navigating the ever-evolving geopolitical landscape. Collaborative efforts on defence projects not only enhance the EU's technological prowess but also contribute to fostering stronger diplomatic ties and alliances, reinforcing the region's position on the international stage.

Innovation should be pursued ethically to ensure that emerging military technologies adhere to the principles of responsible innovation. Member States must prioritise the development of technologies that align with international norms, human rights standards, and legal frameworks. This commitment to ethical practices will not only enhance the legitimacy of the EU's defence initiatives but also mitigate potential risks and concerns associated with the deployment of advanced military capabilities.

Furthermore, societal engagement should be a central tenet of the EU's approach to developing military technologies. Transparency, public discourse, and civil society's involvement in decision-making processes are vital for fostering public trust

and ensuring that technological advancements align with the values and expectations of EU citizens. By engaging the public, Member States can address concerns related to the ethical implications of military technologies and garner support for strategic initiatives.

As EU Member States chart their courses in emerging military technologies, they must remain anchored in the principles of responsible innovation, international cooperation, and societal engagement. These pillars will serve as the foundation for the future, in which military technologies will contribute to the interests of peace, stability, and shared prosperity in the European Union and beyond.

References

Aashish, P. (2023) 'What Is Space Tech? – Use Cases, Examples, & Future', *Feedough*, 7 August 2023. [Online]. Available at: https://www.feedough.com/what-is-space-tech/ (Accessed: 23 February 2024).

Adams, E. (2008) 'How it works: The Flying Laser Cannon', *Popular Science*, 14 March 2008. [Online]. Available at: https://www.popsci.com/military-aviation-space/article/2008-03/how-it-works-airborne-laser-cannon/ (Accessed: 23 February 2024).

Agrawal, G.P. (2002) *Fiber-Optic Communication Systems*. 3rd edn. New York: Wiley Interscience; https://doi.org/10.1002/0471221147.

Altgilbers, L.L., Brown, M.D.J., Grishnaev, I., Novac, B.M., Smith, I.R., Thach, I., Tkach, Y. (2000) *Magnetocumulative Generators*. New York: Springer.

Anderson, M., Anderson, S.L. (2007) 'Machine Ethics', *AI & Society*, 22(4), pp. 477–493.

Andrews, L.C., Philips, R.L. (2005) *Laser Beam Propagation Through Random Media*. 2nd edn. Bellingham, WA: SPIE Press; https://doi.org/10.1117/3.626196.

Appleby, R., Wallace, H.B., Wallace, B. (2007) 'Stanfoff detection of weapons and contraband in the 100 GHz to 1 THz region', *IEEE Transactions on Antennas and Propagation*, 55(11), pp. 2944–2956; https://doi.org/10.1109/TAP.2007.908543.

Arkin, R.C. (2009) *Governing Lethal Behavior in Autonomous Robots*. New York: CRC Press; https://doi.org/10.1201/9781420085952.

Axe, D. (2019) 'How the U.S. Is Quietly Winning the Hypersonic Arms Race', *The Daily Beast*, 16 January 2019. [Online]. Available at: https://www.thedailybeast.com/how-the-us-is-quietly-winning-the-hypersonic-arms-race/ (Accessed: 23 February 2024).

Barrett, B. (2018) 'Lawmakers Can't Ignore Facial Recognition's Bias Anymore', *Wired*, 26 July 2018. [Online]. Available at: https://www.wired.com/story/amazon-facial-recognition-congress-bias-law-enforcement/ (Accessed: 23 February 2024).

Bendett, S. (2017) 'Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems', *The Strategy Bridge*, 12 December 2017. [Online]. Available at: https://thestrategybridge.org/the-bridge/2017/12/12/red-robots-rising-behind-the-rapid-development-of-russian-unmanned-military-systems (Accessed: 23 February 2024).

Bickerton, Ch., Brack, N., Coman, R., Crespy, A. (2022) 'Conflicts of sovereignty in contemporary Europe: a framework of analysis', *Comparative European Politics*, 20(2), pp. 1–18.

Borrie, J., Dowler, A., Podvig, P. (2019) *Hypersonic Weapons: A Challenge and Opportunity for Strategic Arms Control*. New York: United Nations Office for Disarmament Affairs and the United Nations Institute for Disarmament Research; https://doi.org/10.37559/WMD/19/hypson1.

Bostrom, N. (2014) *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press.

Chakraborty, E. (2021) 'Robotics And Autonomous Systems: A Comprehensive Playbook For Science Students', *Techiescience.com*, 6 January 2021. [Online]. Available at: https://techiescience.com/robotics-and-autonomous-systems/?utm_content=cmp-true (Accessed: 23 February 2024).

China State Council (2017) 'A Next Generation Artificial Intelligence Development Plan', *Ministry of Science and Technology, Department of International Cooperation*, 15 September. [Online]. Available at: http://fi.china-embassy.gov.cn/eng/kxjs/201710/P020210628714286134479.pdf (Accessed: 23 February 2024).

Cornet, B., Hua, F., Honggang, W. (2020) 'Overview of Quantum Technologies, Standards, and their Applications in Mobile Devices', *GetMobile: Mobile Computing and Communications*, 24(4), pp. 5–9; https://doi.org/10.1145/3457356.3457358.

Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States (2017) OJ L 331, 14 December 2017.

Csernatoni, R. (2021) 'The EU's Defense Ambitions: Understanding the Emergence of a European Defense Technological and Industrial Complex', *Carnegie Europe*, 6 December 2021. [Online]. Available at: https://carnegieendowment.org/research/2021/12/the-eus-defense-ambitions-understanding-the-emergence-of-a-european-defense-technological-and-industrial-complex?lang=en&center=europe (Accessed: 23 February 2024).

CSET (2021) 'Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035', *Xinhua News Agency*, 12 March 2021. [Online]. Avaialable at: https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf (Accessed: 3 March 2024).

Defense Innovation Board (2019) 'AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense'. [Online]. Available at: https://media.defense.gov/2019/Oct/31/2002204458/1/1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF (Accessed: 12 February 2024).

Defense Intelligence Agency (2019) 'Challenges to Security in Space', January 2019. [Online]. Available at: https://aerospace.csis.org/wp-content/uploads/2019/03/20190101_ChallengestoSecurityinSpace_DIA.pdf (Accessed: 23 February 2024).

Department of Commerce (2020) 'Addition of Entities to the Entity List, and Revision of Entries on the Entity List' *Federal Register*, 22 December. [Online]. Available at: https://www.federalregister.gov/documents/2020/12/22/2020-28031/addition-of-entities-to-the-entity-list-revision-of-entry-on-the-entity-list-and-removal-of-entities (Accessed: 14 February 2024).

Department of Defense (2012) 'Directive 3000.09 – Autonomy in Weapon Systems', *Office of the Under Secretary of Defense for Policy*, 21 November 2012.

Department of Defense (2018) 'Summary of the 2018 National Defense Strategy of The United States of America'. [Online]. Available at: https://dod.defense.gov/portals/1/documents/pubs/2018-national-defense-strategy-summary.pdf (Accessed: 23 February 2024).

Duignan, B., Leong, E. (2023) 'Inventors and Inventions of the Industrial Revolution', *Britannica*, 31 August 2023. [Online]. Available at: https://www.britannica.com/list/inventors-and-inventions-of-the-industrial-revolution (Accessed: 23 February 2024).

European Commission (2021) 'Proposal for a regulation of the European Parliament and of the Council, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts' COM/2021/206 final, Brussels, 21 April 2021.

European Commission (2022) 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)' COM(2022) 46 final, Brussels, 8 February 2022.

European Defence Agency (2017) '10 Upcoming Disruptive Defence Innovations', *European Defence Matters*, 2017/14. [Online]. Available at: https://eda.europa.eu/docs/default-source/eda-magazine/edm-issue-14_web.pdf (Accessed: 23 February 2024).

European Defence Agency (2019) 'Overarching Strategic Research Agenda (OSRA)', 25 March. [Online]. Available at: https://eda.europa.eu/docs/default-source/eda-factsheets/2019-03-25-factsheet-osra (Accessed: 24 February 2024).

European Parliament (2021) 'Big data: definicja, korzyści, wyzwania (infografika)' [Big Data: Definition, Benefits, Challenges (Infographic)], 17 February 2021. [Online]. Available at: https://www.europarl.europa.eu/topics/pl/article/20210211STO97614/big-data-definicja-korzysci-wyzwania-infografika (Accessed: 14 December 2023).

Fediushko, D., Novichkov, N. (2021) *The combat use of unmanned aerial vehicles in Nagorno-Karabakh*. Helsinki: Status.

Freedberg, Jr., S.J. (2020) 'Army Ramps Up Funding for Laser Shield, Hypersonic Sword', *Breaking Defense*, 28 February 2020. [Online]. Available at: https://breakingdefense.com/2020/02/army-ramps-up-funding-for-laser-shield-hypersonic-sword/ (Accessed: 23 February 2024).

Gallo, M.E., Sarata, A.K., Sargent, Jr., J.F., Cowan, T. (2018) 'Advanced Gene Editing: CRISPR-Cas9', *Congressional Research Service*, 7 December 2018. [Online]. Available at: https://crsreports.congress.gov/product/pdf/R/R44824/6 (Accessed: 23 February 2024).

Gertz, B. (2018) 'China Reveals Test of New Hypersonic Missile', *The Washington Free Beacon*, 10 August 2018. [Online]. Available at: https://freebeacon.com/national-security/chinas-reveals-test-new-hypersonic-missile/ (Accessed: 23 February 2018).

Gregory, C.A. (2017) 'Putin and Musk Are Right: Whoever Masters AI Will Run the World', *CNN*, 5 September 2017. [Online]. Available at: https://edition.cnn.com/2017/09/05/opinions/russia-weaponize-ai-opinion-allen/index.html (Accessed: 23 February 2024).

Hadley, G. (2021) 'Kendall: China Has Potential to Strike Earth From Space', *Air&Space Forces Magazine*, 20 September 2021. [Online]. Available at: https://www.airandspaceforces.com/global-strikes-space-china-frank-kendall/ (Accessed: 23 February 2024).

Hagel, Ch. (2014) '"Defense Innovation Days" Opening Keynote (Southeastern New England Defense Industry Alliance)', *U.S. Department of Defense*, 3 September 2014. [Online]. Available at: https://www.defense.gov/News/Speeches/Speech/Article/605602/ (Accessed: 14 January 2024).

Hendrickx, B. (2020) 'Peresvet: a Russian mobile laser system to dazzle enemy satellites', *The Space Review*, 15 June 2020. [Online]. Available at: https://www.thespacereview.com/article/3967/1 (Accessed: 23 February 2024).

Hicks, K.H. (2021) 'Implementing Responsible Artificial Intelligence in the Department of Defense', 26 May. [Online]. Available at: https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/IMPLEMENTING-RESPONSIBLE-ARTIFICIAL-INTELLIGENCE-IN-THE-DEPARTMENT-OF-DEFENSE.PDF (Accessed: 23 February 2024).

ISO (2021) 'Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles' ISO/SAE PAS 22736:2021(en), August 2021. [Online]. Available at: https://www.iso.org/standard/73766.html (Accessed: 21 December 2023).

Joint Chiefs of Staff (2020) 'Joint Electromagnetic Spectrum Operations' Joint Publication 3-85, 22 May. [Online]. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf (Accessed: 23 February 2024).

Jonson, J. (2019) 'Artificial intelligence & future warfare: implications for international security', *Defense & Security Analysis*, 35(2), pp. 147–169; https://doi.org/10.1080/14751798.2019.1600800.

Kania, E.B. (2017) *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*. Washington, DC: Center for a New American Security. [Online]. Available at: https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf (Accessed: 23 February 2024).

Kania, E.B., Costello, J. (2018) 'Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership', *Center for a New American Security*, 12 September 2018. [Online]. Available at: https://www.cnas.org/publications/reports/quantum-hegemony (Accessed: 23 February 2024).

Konaev, M., Imbrie, A., Fedasiuk, R., Weinstein, E., Sedova, K., Durham, J. (2021) 'Headline or Trend Line? Evaluating Chinese-Russian Collaboration in AI', *Center for Security and Emerging Technology*, August 2021. [Online]. Available at: https://cset.georgetown.edu/publication/headline-or-trend-line/ (Accessed: 23 February 2024).

Leonelli, M. (2021) 'Simulation and Modelling to Understand Change', *School of Human Sciences and Technology*, Lecture notes. [Online]. Available at: https://bookdown.org/manuele_leonelli/SimBook/ (Accessed: 12 February 2024).

Lucas, N.J. (2016) 'Lethal Autonomous Weapon Systems: Issues for Congress', *Congressional Research Service*, 14 April 2016. [Online]. Available at: https://crsreports.congress.gov/product/details?prodcode=R44466 (Accessed: 23 February 2024).

McMahon, R. (2021) *The Cold War: A Very Short Introduction*. 2nd edn. Oxford: Oxford Academic; https://doi.org/10.1093/actrade/9780198859543.001.0001.

Merriam-Webster Dictionary (no date) 'Autonomy'. [Online]. Available at: https://www.merriam-webster.com/dictionary/autonomy (Accessed: 14 February 2024).

Miklush, L. (no date) 'Sensory system: Structure and function', *Osmosis*. [Online]. Available at: https://www.osmosis.org/learn/Sensory_system:_Structure_and_function (Accessed: 23 February 2024).

Miller, J.N., Rose, F.A. (2018) 'Bad Idea: Space-Based Interceptors and Space-Based Directed Energy Systems', *Defense360*, 13 December 2018. [Online]. Available at: https://defense360.csis.org/bad-idea-space-based-interceptors-and-space-based-directed-energy-systems/ (Accessed: 23 February 2024).

Mizokami, K. (2019) 'The U.S. Army Plans To Field the Most Powerful Laser Weapon Yet', *Popular Mechanics*, 7 August 2019. [Online]. Available at: https://www.popularmechanics.com/military/weapons/a28636854/powerful-laser-weapon/ (Accessed: 23 February 2024).

Mizokami, K. (2020) 'The Air Force Mobilizes Its Laser and Microwave Weapons Abroad', *Popular Mechanics*, 9 April 2020. [Online]. Available at: https://www.popularmechanics.com/military/weapons/a32083799/laser-microwave-weapons/ (Accessed: 23 February 2024).

National Security Commission on Artificial Intelligence (2021) 'Final Report', March 2021. [Online]. Available at: https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (Accessed: 28 February 2024).

Nishawn, S.S. (2020) 'Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition', *Congressional Research Service*, 4 June 2020. [Online]. Available at: https://sgp.fas.org/crs/intel/R46389.pdf (Accessed: 23 February 2024).

Novichkov, N. (2018) 'Airshow China 2018: CASIC's LW-30 laser weapon system breaks-cover', *Jane's Defence Weekly*, 9 November 2018.

Office of the President of the Russian Federation (2019) 'Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation', *Center for Security and Emerging Technology*, 10 October. [Online]. Available at: https://cset.georgetown.edu/publication/decree-of-the-president-of-the-russian-federation-on-the-development-of-artificial-intelligence-in-the-russian-federation/ (Accessed: 28 December 2023).

Office of the Secretary of Defense (2019) 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019', 2 May. [Online]. Available at: https://media.defense.gov/2019/May/02/2002127082/1/1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf (Accessed: 27 December 2023).

Office of the Under Secretary of Defense (2021) 'Defense Budget Overview', *United States Department of Defense*, May 2021. [Online]. Available at: https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Budget_Request_Overview_Book.pdf (Accessed: 23 February 2024).

Pahwa, A. (2023) 'What Is Space Tech? – Use Cases, Examples, & Future', *Feedough*, 7 August 2023. [Online]. Available at: https://www.feedough.com/what-is-space-tech/ (Accessed: 23 February 2024).

Pariseau-Legault, P., Holmes, D., Murray, S.J., (2019) 'Understanding human enhancement technologies through critical phenomenology', *Nursing Philosophy*, 20(1); https://doi.org/10.1111/nup.12229.

Patrick, M.C., Ryan, D.N. (2020) 'Countering China's Laser Offensive', *The Diplomat*, 2 April 2020. [Online]. Available at: https://thediplomat.com/2020/04/countering-chinas-laser-offensive/ (Accessed: 14 February 2024).

Public Law No. 114-328 (2016) – *National Defense Authorization Act for Fiscal Year 2017*, U.S. Government Publishing Office, 23 December 2016.

Public Law No. 115-232 (2018) *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, U.S. Government Publishing Office, 13 August 2018.

Public Law No. 115-368 (2018) *National Quantum Initiative Act*, U.S. Government Publishing Office, 21 December 2018.

Public Law No. 116-283 (2021) *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, U.S. Government Publishing Office, 1 January 2021.

Public Law No. 116-92 (2019) *National Defense Authorization Act for Fiscal Year 2020*, U.S. Government Publishing Office, 20 December 2019.

Quirin, S. (2019) 'Russia joins race to make quantum dreams a reality', *Nature*, 17 December 2019. [Online]. Available at: https://www.nature.com/articles/d41586-019-03855-z (Accessed: 23 February 2024).

Raitasalo, J. (2019) 'Hypersonic Weapons are No Game-Changer', *The National Interest*, 5 January 2019. [Online]. Available at: https://nationalinterest.org/blog/buzz/hypersonic-weapons-are-no-game-changer-40632 (Accessed: 23 February 2024).

Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092 (Text with EEA relevance) (2021) OJ L 170, 12 May 2021.

Rouse, M. (no date) 'Information and Communication Technology (ICT)', *Technopedia*. [Online]. Available at: https://www.techopedia.com/definition/24152/information-and-communications-technology-ict (Accessed: 23 February 2024).

Russian Federation (no date) 'BIO2020: Summary of the State Coordination Program for the Development of Biotechnology in the Russian Federation'. [Online]. Available at: http://biotech2030.ru/wp-content/uploads/2017/05/BIO2020_Summary.pdf (Accessed: 23 February 2024).

Saracino, P. (2019) 'Battlefield medicine', *Encyclopedia Britannica*, 6 November 2019. [Online]. Available at: https://www.britannica.com/science/battlefield-medicine (Accessed: 23 February 2024).

Sayler K.M., DiMascio, J., Feickert, A., O'Rourke, R. (2023) 'Department of Defense Directed Energy Weapons: Background and Issues for Congress', *Congressional Research Service*, 22 August 2023. [Online]. Available at: https://crsreports.congress.gov/product/details?prodcode=R46925 (Accessed: 23 February 2024).

Sayler, K.M. (2020) 'Artificial Intelligence and National Security', *Congressional Research Service*, 10 November 2020. [Online]. Available at: https://crsreports.congress.gov/product/details?prodcode=R45178 (Accessed: 23 February 2024).

Sayler, K.M. (2024a) 'Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems', *Congressional Research Service*, 1 February 2024. [Online]. Available at: https://crsreports.congress.gov/product/pdf/IF/IF11150/11 (Accessed: 23 February 2024).

Sayler, K.M. (2024b) 'Hypersonic Weapons: Background and Issues for Congress', *Congressional Research Service*, 9 February 2024. [Online]. Available at: https://crsreports.congress.gov/product/details?prodcode=R45811 (Accessed: 23 February 2024).

Sayler, K.M., McCall, S.M., Reed, Q.A. (2020) 'Hypersonic Missile Defense: Issues for Congress', *Congressional Research Service*, 17 August 2020. [Online]. Available at: https://crsreports.congress.gov/product/pdf/IF/IF11623/1 (Accessed: 23 February 2024).

Scharre, P. (2015) 'Directed-Energy Weapons: Promise and Prospects', *Center for a New American Security*, April 2015.

Science & Tech (no date) *Britannica*. [Online]. Available at: https://www.britannica.com/Science-Tech (Accessed: 14 January 2024).

Seapower Staff (2021) 'Lockheed Martin's HELIOS Shipboard Laser Being Tested at Wallops Island', *Seapower*, 1 August 2021. [Online]. Available at: https://seapowermagazine.org/lockheed-martins-helios-shipboard-laser-being-tested-at-wallops-island/ (Accessed: 23 February 2024).

Seldin, J. (2022) 'What Are Hypersonic Weapons and Who Has Them?', *VOA News*, 22 March 2022. [Online]. Available at: https://www.voanews.com/a/what-are-hypersonic-weapons-and-who-has-them-/6492459.html (Accessed: 12 February 2024).

Sevastopulo, D., Hille, K. (2021) 'China tests new space capability with hypersonic missile', *Financial Times*, 16 October 2021. [Online]. Available at: https://www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb (Accessed: 23 February 2024).

Simonite T. (2017) 'For Superpowers, Artificial Intelligence Fuels New Global Arms Race', *Wired*, 8 September 2017. [Online]. Available at: https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/ (Accessed: 23 February 2024).

Storage Technology Definitions (no date) *TechTarget*. [Online]. Available at: https://www.techtarget.com/searchstorage/definitions (Accessed: 12 March 2024).

Tate, A. (2020) 'China aiming to procure airborne laser-based weapon pod', *Jane's Defence Weekly*, 8 January 2020.

Theohary, C.A. (2023) 'Defense Primer: Information Operations', *Congressional Research Service*, 14 December 2023. [Online]. Available at: https://crsreports.congress.gov/product/details?prodcode=IF10771 (Accessed: 23 February 2024).

Tucker, P. (2019) 'SecDef: China Is Exporting Killer Robots to the Mideast', *Defense One*, 5 November 2019. [Online]. Available at: https://www.defenseone.com/technology/2019/11/secdef-china-exporting-killer-robots-mideast/161100/ (Accessed: 23 February 2024).

U.S. Government (2018) 'Humanitarian Benefits of Emerging Technologies in the Area of Lethal Autonomous Weapons', 3 April. [Online]. Available at: https://ogc.osd.mil/Portals/99/Law%20of%20War/Practice%20Documents/US%20Working%20Paper%20-%20Humanitarian%20benefits%20of%20emerging%20technologies%20in%20the%20area%20of%20LAWS%20-%20CCW_GGE.1_2018_WP.4_E.pdf?ver=O0lg6BIxsFt57nrOuz3xHA%3D%3D (Accessed: 27 December 2023).

U.S. Government Accountability Office (2018) 'National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies', December 2018. [Online]. Available at: https://www.gao.gov/assets/700/695981.pdf (Accessed: 23 February 2024).

U.S.-China Economic and Security Review Commission (2014) 'Annual Report', November 2014. [Online]. Available at: https://www.uscc.gov/sites/default/files/annual_reports/Complete%20Report.PDF (Accessed: 27 December 2023).

U.S.-China Economic and Security Review Commission (2015) 'Annual Report', November 2015. [Online]. Available at: https://www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF (Accessed: 27 December 2023).

U.S.-China Economic and Security Review Commission (2017) 'Annual Report', November 2017. [Online]. Available at: https://www.uscc.gov/sites/default/files/2019-09/2017_Annual_Report_to_Congress.pdf (Accessed: 27 December 2023).

U.S.-China Economic and Security Review Commission (2018) 'Annual Report', November 2018. [Online]. Available at: https://www.uscc.gov/sites/default/files/annual_reports/2018%20Annual%20Report%20to%20Congress.pdf (Accessed: 27 December 2023).

UN General Assembly (1977) 'Prohibition of the development and manufacture of new types of weapons of mass destruction and new systems of such weapons' A/RES/32/84[B], 12 December 1977.

United Nations (2018) 'Position Paper Submitted by China' CCW/GGE.1/2018/WP.7, Geneva, 11 April. [Online]. Available at: https://documents.un.org/doc/undoc/gen/g18/102/09/pdf/g1810209.pdf (Accessed: 23 February 2024).

United Nations (2019) 'Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems' CCW/GGE.1/2019/3, Geneva, 25 September. [Online]. Available at: https://documents.unoda.org/wp-content/uploads/2020/09/CCW_GGE.1_2019_3_E.pdf (Accessed: 23 February 2024).

Varlamov, A.A., Rimshin, V.I., Tverskoi, S.Y. (2018) 'Security and destruction of technical systems', *IFAC*-PapersOnLine, 51(30), pp. 808–811; https://doi.org/10.1016/j.ifacol.2018.11.190.

Wahab, M.A. (2014) '6.03 – Manual Metal Arc Welding and Gas Metal Arc Welding' in Hashmi, S., Batalha, G.F., Van Tyne, C.J., Yilbas, B. (eds.) *Comprehensive Materials Processing*. Amsterdam: Elsevier, pp. 47–76; https://doi.org/10.1016/B978-0-08-096532-1.00610-5.

Will, K. (2016) 'How to Fix Silicon Valley's Sexist Algorithms', *MIT Technology Review*, 23 November 2016. [Online]. Available at: https://www.technologyreview.com/2016/11/23/155858/how-to-fix-silicon-valleys-sexist-algorithms/?gad_source=1&gbraid=0AAAADgO_miCq58JhpgGRAIoJgZXEYxdA&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZhxfWsGkEnQppwfjmB4GycQECHy2HNeeurBTW5gm4G49NZeRpkoXgaApXIEALw_wcB (Accessed: 23 February 2024).

Woolf, A.F. (2021) 'Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues', *Congressional Research Service*, 9 February 2021. [Online]. Available at: https://crsreports.congress.gov/product/details?prodcode=R41464 (Accessed: 23 February 2024).

Work, B. (2014) 'National Defense University Convocation', *U.S. Department of Defense*, 5 August 2014. [Online]. Available at: https://www.defense.gov/News/Speeches/Speech/Article/605598/ (Accessed: 14 January 2024).

Yeung, J. (2018) 'China claims to have successfully tested its first hypersonic aircraft', *CNN World*, 7 August 2018. [Online]. Available at: https://edition.cnn.com/2018/08/07/china/china-hypersonic-aircraft-intl/index.html (Accessed: 23 February 2024).

Zakheim, R., Karako, T. (2019) 'China's Hypersonic Missile Advances and U.S. Defense Responses', *Hudson Institute*, 11 March 2019. [Online]. Available at: https://s3.amazonaws.com/media.hudson.org/China%27s%20Hypersonic%20Missile%20Advances%20and%20U.S.%20Defense%20Responses%20-%20Final%20Transcript.pdf (Accessed: 23 February 2024).

Disruptive Defence Innovations Ahead! (no date) *European Defence Matters*. [Online]. Available at: https://eda.europa.eu/webzine/issue14/cover-story/disruptive-defence-innovations-ahead (Accessed: 24 February 2024).

Gliding missiles that fly faster than Mach 5 are coming (2019) *The Economist*, 6 April 2019. [Online]. Available at: https://www.economist.com/science-and-technology/2019/04/06/gliding-missiles-that-fly-faster-than-mach-5-are-coming (Accessed: 3 January 2024).

Part II

THE CSDP AND LAW

Chapter 4

Common Security and Defence Policy: A Legal Framework for Developing the European Defence Industry

Krzysztof Masło

Abstract

The European Union's (EU) Common Security and Defence Policy (CSDP) is a component of its Common Foreign and Security Policy (CFSP). It was established in the Maastricht Treaty on European Union, which included a provision for the gradual introduction of a common defence policy that could eventually lead to a common defence framework.

The CFSP emerged from the need to enhance the EU's political identity on the international arena and assert Europe's independence in the post-Cold War era. Simultaneously, it remains one of the few areas of competence that exclusively belongs to Member States, where proposals to deepen integration processes have met with lukewarm responses. However, the Russo-Ukrainian war has prompted the European forum to strengthen cooperation between Member States, particularly in the defence industry sector.

The CSDP is regulated only by the Treaty on EU (TEU), while other EU policies are governed by the Treaty on the Functioning of the EU (TFEU). The architects of the Lisbon reform aimed to underscore the distinctiveness of the CSDP from other EU policies, as demonstrated by its legal instruments, decision-making mechanisms, and the nature of EU competences. Cooperation under the CSDP does not fit neatly within the traditional treaty rules governing the division of competences between the EU and its Member States. Fundamental competences in the field of security policy are reserved for Member States, which result from both the TEU and the unambiguous content of Declaration No. 13 on the CFSP.

Krzysztof Masło (2024) 'Common Security and Defence Policy: A Legal Framework for Developing the European Defence Industry'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 161–211. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_4

The CSDP's intergovernmental nature CSDP determines its institutional implementation. It is defined and implemented by intergovernmental EU institutions, particularly the European Council and the Council. The High Representative supported by the European External Action Service and Member States play a key role in its implementation, drawing on both EU and national funds. The competences of the EU's supranational institutions, particularly the Court of Justice of European Union, are strictly limited in this area.
The relationship between the North Atlantic Treaty Organization and the EU was institutionalised in the early 21st century, building on initiatives from the 1990s aimed at promoting greater European responsibility in defence matters.

Keywords: Common Foreign and Security Policy (CFSP), CSDP legal basis, Court of Justice of EU (CJEU), decision-making mechanism in the CSDP, North Atlantic Treaty Organization (NATO), Treaty on European Union (TEU)

1. Introduction

The legal framework of the European Union's (EU) Common Security and Defence Policy (CSDP), a component of its Common Foreign Security Policy (CFSP), CSDP was first established in the Maastricht Treaty on EU (TEU) on 7 February 1992, although political-level cooperation in foreign areas has been in existence since the 1970s.

The CSDP stemmed from the need to strengthen EU's political identity on the international stage and emphasise Europe's independence post-Cold War. Simultaneously, it is one of the few areas of competence belonging to Member States where proposals to deepen integration processes have been met with a lukewarm response from Member States. However, the Russia–Ukraine war forced European forums to strengthen relations between Member States, particularly in the field of CSDP.

While CSDP does not explicitly distinguish between CFSP and Common Security and Defence Policy (CSDP), TEU specifically mentions CSDP in Article 42(2) TEU. It states that CSDP covers the progressive definition of the EU's CSDP and further specifies that it will lead to a common defence if the European Council, acting unanimously, decides so. Therefore, the TEU makes a clear distinction between CSDP and common defence; common defence is an element of the CSDP, although its activation depends on the European Council's political decisions. Conversely, CSDP has gradually been defined.

As TEU does not define CSDP, it is difficult to distinguish between provisions relating to defence policy and security. This chapter focuses on the broader legal foundations of CSDP. First, I introduce the historical development of legal regulation of the CSDP. Subsequently, I characterise the legal foundations of CSDP and the

decision-making process. Given the intergovernmental character of CSDP cooperation, I briefly refer to the issue of sovereignty. Subsequently, I present the institutional structure of CSDP and its relationship with the North Atlantic Treaty Organization (NATO).

2. Historical development of CSDP

The EU established international relations in the 1950s – initially, as a purely economic project operating within three communities: the European Coal and Steel Community (ECSC), European Economic Community (EEC) and European Atomic Energy Community. The success of ECSC encouraged Member States to deepen integration within political–military areas. Accordingly, the legal aspects of integration in the political–military field are the subject of this subsection. The emergence and development of European Political Cooperation (EPC) will be discussed in another part of the book.

2.1. Initial proposals for the establishment of European Defence Community and European Political Community

In 1950, Winston Churchill proposed to the Parliamentary Assembly of the Council of Europe the establishment of a European army commanded by a European Defence Minister.[1] In response, an announcement was made by French Prime Minister Rene Pleven in October 1950 regarding a plan to create a European Defence Community (EDC).[2]

Negotiations on the proposal began on 15 February 1951, and on 27 May 1952, representatives of ECSC Member States signed a treaty in Paris to establish EDC.[3] The EDC aimed to secure Europe against aggression and maintain peace. Therefore, it is a typical military alliance.[4] The treaty also contained a *casus foederis* (commitment to common defence, Article 2(3) of the treaty). It established a European army with 40 national divisions comprising 13,000 uniformed soldiers each. It comprised an integrated land, air and naval force of Member States at the corps level (Articles 9–18). The treaty provided for the establishment of the institutional structure of the future community and envisaged the creation of a Commissionariat (Articles 19–32), Council of Defence Ministers (Articles 39–50), Assembly (Articles 33–38) and a Court (Articles 51–67).

1 Schmidt, 2020, p. 32.
2 Koutrakos, 2013, p. 6.
3 Treaty text available at: https://aei.pitt.edu/5201/1/5201.pdf (Accessed: 21 January 2024).
4 Koutrakos, 2013, p. 7.

The project to create EDC was met with reservations from European capitals. However, it won the approval of the German government and the United States. In France, support for a joint army declined and the balance of political power led the National Assembly of France to reject the proposal to ratify the treaty on 30 August 1954.[5] Consequently, work on the treaty was also abandoned in other countries.[6]

Corresponding to the creation of EDC, efforts were being made towards the realisation of political integration within the framework of the European Political Community (EPC). In July 1952, the ECSC Assembly drafted a statute for establishing a new community. Belgian politician Paul Henri Spaak led the preparation to draft the treaty establishing ECSC; the draft treaty was prepared in 1953.[7] This gave the new community a supranational character and established an institutional structure. The organs of the EPC are the Parliament, Executive Council, President, Court of Justice and the Economic and Social Council. The Parliament consists of two chambers; the People's Chamber is elected by universal suffrage and European Senate by the national Parliaments of EPC Member States. A President was to be elected by Senate. The Executive Council took over the functions of the Council of Ministers of the ECSC and was responsible for the People's Chamber and the President. The Court of Justice (CJ) is the judicial organ of ECSC.

Considering that the French National Assembly rejected the treaty establishing EDC, work on establishing EPC was also interrupted.[8]

2.2. Establishment and functions of Western European Union

Meanwhile, the failure to establish EDC and EPC stalled the process of European integration in the political–military field, and Western European states decided to develop less-intrusive defence alliances in their sovereign rights. Principally, a decision was made to rebuild the 1948 Brussels Treaty and the Western Union was established on its basis.

The Brussels Treaty, signed on 17 March 1948 by France, Benelux countries and the United Kingdom, originally concerned political, military and economic cooperation.[9] The Treaty was in response to explicit requests from the United States for European partners to institutionalise their efforts to ensure effective self-defence in the face of threats from the Soviet Union and the emerging bloc of Communist States. The treaty was concluded 50 years ago and was open to any country (Article IX). In addition to economic and social cooperation, the treaty contained provisions on mutual security. In the preamble, it was written that they would assist each other in the maintenance of international peace and security. Furthermore, Article IV

5 Butler, 2021, p. 21.
6 Neuhold, 2013, p. 1.
7 Mik, 2000, p. 36.
8 Butler, 2021, p. 22.
9 *The Treaty of Economic, Social and Cultural Collaboration and Collective Self-Defence*, 1948; in: Bloed and Wessel, 1994, pp. 1–6.

enshrines an alliance clause pledging assistance in the event of an armed attack on either party's territory.

> Should one of the Highly Contracting Parties be subjected to armed aggression in Europe, the other Parties shall, in accordance with the provisions of Article 51 of the Charter of the United Nations, render aid and assistance to it by all means available to them, whether military or otherwise.[10]

The steps taken under Article IV were immediately reported to the UN Security Council (Article V). The Brussels Treaty provided for the creation of a Western Union with its own bodies, including military groups (Article VII), which was the first intergovernmental organisation to be established in Western Europe after the Second World War.

The failure of EDC and EPC changed the perception of Western Union. Simultaneously, the 1951 NATO began functioning based on the 1949 Washington Treaty. The aims of NATO were relatively similar to those of the Western Union. Britain took the initiative to admit West Germany to the Brussels Treaty as late as 1954. The Paris Accords, amending the Brussels Treaty of 1948, were signed on 23 October 1954.[11] Accordingly, Germany and Italy joined the Western Union (Article 1) and the name of the organisation changed to Western European Union (WEU). The Paris Agreement ended occupational regime and restored the sovereignty of the Federal Republic of Germany by regulating the presence of foreign troops on German territory.

A provision was added to the preamble of the Brussels Treaty, stating that Member States would assist each other in ensuring international peace and security by refraining from aggression. This provision legitimised possible actions of WEU outside the territories of its members, while creating the need for the organisation's security policy to consider two dimensions: the defence of Member States' territories against external aggression and a defence policy in a broader sense, considering areas beyond the borders of WEU members.[12] The preamble to the modified Brussels Treaty also defined the tasks of WEU as the defence of democratic values, human rights and civil liberties, constitutional traditions and respect for the law.

Article IV of the modified Brussels Treaty institutionalised the WEU's cooperation with NATO. It provided that, to avoid unnecessary duplication of NATO military structures, the WEU Council and its agencies would consult with NATO military authorities on matters of military nature. These provisions gave the WEU the role of the European pillar of the transatlantic security system, which had been demanded by the United States from the beginning. The WEU was thus, a non-self-dependent

10 Ibid.

11 *Protocol Modifying and Completing the Brussels Treaty (Western European Union)*, 1954; in: Bloed and Wessel, 1994, pp. 7–15.

12 Macalister-Smith and Gebhard, 2013, p. 46.

organisation militarily from the beginning, and its creation did not fundamentally change the political and military situation on the continent.

Despite the establishment of links between the WEU and NATO, the modified Brussels Treaty did not abandon the alliance clause obliging WEU Member States to provide military or other assistance to any party in the event of armed aggression (Article V).

The modified Brussels Treaty equipped the WEU with the institutional structure necessary to fulfil its tasks. Article VIII established the WEU Council as the body set up to strengthen peace and security, enhance unity among states and promote progressive integration of Europe by strengthening cooperation among States that are Parties to the treaty. The WEU Council was supposed to be a forum for considering all issues covered by the treaty. It could be convened at any time, at the request of any Member State, in the event of a threat to peace or economic stability, regardless of where the threat occurred. Article VIII also announced the creation of an Arms Control Agency, whose tasks are defined in Protocol IV.

Article VIII of the modified Brussels Treaty also determined the voting method in the WEU Council, introducing unanimity as a rule.

The modified Brussels Treaty provided a formal legal basis for the coordination of Western European States' actions in the field of defence and international security in the face of escalating threat posed by the Cold War and Western Europe's progressive confrontation with the United States–Soviet Union. It was an expression of the willingness of Western European allies to contribute to the development of defence capabilities and was intended to demonstrate that European States did not intend to rely solely on the protective umbrella of U.S. forces. The inclusion of an alliance clause in the provisions of the Brussels Treaty gave it the character of a defence pact, obliging Parties to pursue a coordinated and solidarity-based security policy and seek ways to jointly counter threats.

Although the purpose of the modified Brussels Treaty was to equip WEU with real competencies regarding security matters, the international situation led it to abandon its efforts to strengthen European security rather quickly. Faced with the growing military potential of the Soviet Union and its satellite states, Western Europe based its security on its alliance with the United States and the development of NATO rather than on developing its own collective defence organisation.[13] Admittedly, the WEU's exclusive competence includes arms control within the framework of the Arms Control Agency. However, in reality, it was only applied in Germany and terminated by a Council decision in 1987.[14] In May 1972, efforts to convene the WEU Council sessions were abandoned and the organisation suspended the exercise of its core functions.[15]

13 Gadkowski et al., 2019, p. 88.
14 Howorth, 2012, pp. 7–8.
15 Schmidt, 2020, p. 36.

It was only in the 1980s and 1990s that an attempt was made to reactivate the WEU and link it to European Communities, and subsequently to the emerging EU. In the 1980s, discussions began to define European security and defence interests.[16] Within the WEU, the issue was considered at a session of the Council of Foreign and Defence Ministers on 23 April 1990 in Brussels.[17] The meeting initiated a discussion that lasted several years on whether the WEU should continue in its present form or be incorporated into the emerging EU.

2.3. Developing defence integration within the EU

A breakthrough in the development of political and defence cooperation between the Member States of European Communities was the signing of the Single European Act (SEA) in 1986.[18] The SEA had two dimensions: revision of existing founding treaties of the three Communities and regulation of EPC, which until then functioned without a treaty.

In the preamble to SEA, signatories declared that they intended to be guided by 'the will to continue the work undertaken on the basis of the Treaties establishing the European Communities and to transform all relations between their States into a European Union, in accordance with the Solemn Declaration of Stuttgart of 19 June 1983'. They declared that they were 'determined to establish a European Union', based on European Communities and EPC, and endow 'the Union with the necessary means to act'. In Article 1, Title I of the Treaty, the signatories also stated that 'the European Communities and European Political Co-operation accept as their objective to make a joint contribution to achieving visible progress towards (the establishment of) the European Union'.

Provisions for cooperation in the foreign-policy sphere are included in Title III of SEA (Article 30 SEA). The SEA contained a general commitment that EEC Member States should jointly endeavour to formulate and implement European foreign policy. It also included the obligation to exchange information between Member States and consult with each other on all foreign policy issues of general interest (Article 30(2)(c)). Furthermore, in accordance with SEA regarding the adoption of its position and national measures, each Member State should take full account of the positions of other partners and appropriately discern the desirability of adopting and implementing common European positions. Member States should endeavour to avoid any action or position that diminishes their effectiveness in international relations (Article 30(2)(d)). Meetings of foreign ministers, also attended by members of the Commission, were held at least four times a year. Foreign Ministers could also consider matters relating to the activities of EPC at EEC Council meetings (Article 30(3a) SEA). EPC Leadership was assigned to the Member State currently holding

16 Howorth, 2012, pp. 7–8.
17 de Waele, 2023, p. 63.
18 *Single European Act*, 1987.

the Presidency of the EEC Council. It is responsible for initiating, coordinating and directing the activities of Member States in the EPC (Article 30(10a-b) SEA).

The inclusion of cooperation in European security matters in the EPC (Article 30(6a) SEA) was groundbreaking. The Member States of European Communities recognised the need to maintain the technological and industrial conditions necessary for their security and cooperated at the national level. However, cooperation in the field of security could not in any manner affect the obligations of certain states of European Communities arising from their membership of NATO and WEU (Article 30(6c) SEA).

The SEA also established a permanent secretariat for EPC, based in Brussels, to assist Presidency in the administrative preparation and implementation of foreign-policy cooperation (Article 30(10g) SEA).

The SEA further confirmed the participation of the Commission and European Parliament in EPC work. The Commission was to be "fully associated" (Article 30(3b) SEA) and the European Parliament "closely associated" with the activities of EPC (Article 30(4) SEA). The European Parliament should also be regularly informed of foreign policy issues dealt with by the EPC, and the latter should consider the European Parliament's foreign policy opinions (Article 30(4) SEA). The Treaty did not extend the jurisdiction of the Court of Justice to EPC (Article 31 SEA).

The signatories of SEA also reserved the possibility of amending the provisions of EPC five years after the entry into force of the agreement (Article 30(12) SEA).

The 1980s and 1990s brought about significant political and economic changes that influenced the expansion of European integration. The collapse of communism and the disintegration of Soviet Union led to the dismemberment of the military structures of the Eastern Bloc, postponing the risk of war on the European continent. Western Europe's economic integration has achieved its goals. The EEC established a customs union in the 1970s and a single market was to be achieved before 1992. Simultaneously, the political importance of European Communities in the international arena was not very high. Against this backdrop, a decision was made in December 1989 to convene an intergovernmental conference to draft a new treaty.[19] From the outset, discussions on strengthening cooperation in the fields of foreign, security and defence policies were extremely controversial.[20] The Member States of European Communities agreed on the text of the Treaty on European Union (TEU) in December 1991. It was signed on 7 February 1992 in Maastricht and came into force on 1 November 1993. In Ireland, France and Denmark, ratification of the treaty required national referenda. The TEU was concluded for an indefinite period.

The TEU ushered in a new phase in the process of European integration.

First, it established the EU, which in legal terms meant changes to the treaties establishing European Communities (the EEC was replaced by European Community) and the introduction of new forms of cooperation between Member States. The EU

19 European Council, 1989.
20 Mik, 2000, p. 60.

was shaped as a structure for cooperation between States of a different nature than traditional international organisations. It was not endowed with legal subjectivity at the international legal level. As history has shown, the EU was intended to be an intermediate stage on the road to full economic, political and monetary integration of European States. The EU is a type of "superstructure" with three pillars:

- Pillar I (economic) comprising the European Community, ECSC and Euratom;
- Pillar II covering CFSP;
- Pillar III representing cooperation in the field of justice and home affairs.[21]

The CFSP provisions in Title V of TEU (‚Provisions on CFSP') were a consequence of a compromise. During deliberations at the Intergovernmental Conference, differences in opinion emerged regarding the nature of CFSP. Some States (Germany, Denmark, Portugal and Greece) agreed that CFSP should be based on inter-State cooperation; meanwhile, France, Belgium, the Netherlands, Luxembourg and Ireland supported giving the policy more autonomy, and in the long run, advocated communitarisation of CFSP.[22] There were also divergent views on defence cooperation, with some states (including Germany, France, Belgium, Luxembourg and Spain) seeking to establish – in some time perspective – CSDP.[23] Others, led by the United Kingdom, demanded respect for their national identities in the defence and preservation of NATO's dominant role in Europe.

As envisaged in TEU, CFSP was to become an expression of the EU's aspiration to raise its profile worldwide. These aspirations are made visible in the EU's objectives. According to Article B, one of EU's objectives was to assert its identity on the international arena, in particular, through CFSP, including ultimately defining a common policy that could lead to common defence. This objective was further detailed in Article J.1; accordingly, the objectives of CFSP include:

- safeguarding EU's common values, fundamental interests and independence;
- strengthening the security of EU and its Member States in all ways;
- preserving peace and strengthening international security in accordance with the principles of the UN Charter, Helsinki Final Act and Paris Charter.
- promoting international cooperation;
- developing and consolidating democracy and rule of law, and respect for human rights and fundamental freedom.

CFSP was equipped with its own legal instruments separate from those of European Communities. The principles and general guidelines of CFSP as defined by the European Council (Article J.8(1) TEU) were fundamental. These were adopted unanimously, but were not legally binding to Member States. The principles and general guidelines could not deal with matters affecting military or defence.

21 de Waele, 2023, p. 34.
22 Lonardo, 2023, p. 50.
23 Ibid.

In implementing the principles and general guidelines, the Council could adopt common positions (Article J.2(2) TEU) or joint actions (Article J.3 TEU) that were binding on Member States. In addition to these legal acts, the TEU established systematic cooperation (Article J.1(3) TEU). However, the legal acts adopted under CFSP were not covered by the fundamental principles developed for the first pillar (principle of primacy of law and direct effect of community law). TEU also contained specific provisions governing its decision-making mechanism, underlining the intergovernmental nature of CFSP. As a rule, all CFSP decisions were made unanimously. The exception was joint actions, which could be adopted by a qualified majority, but only if decided unanimously (Article J.3(2) TEU).

The TEU gave the European Commission and European Parliament limited competences in the development and implementation of CFSP. Notably, it excluded these institutions from legislative processes. Therefore, the creation and application of CFSP legislation was entrusted exclusively to intergovernmental bodies (the European Council and the Council). Furthermore, CFSP was excluded from the jurisdiction of the Court of Justice (Article L).

The TEU did not include many provisions on defence policies. According to Article J.4(1), 'The common foreign and security policy shall include all questions related to the security of the Union, including the eventual framing of a common defence policy, which may in time lead to a common defence'. This provision did not establish any obligations for now, but left it to Member States to take future actions, leading to a common defence. States, therefore, did not agree to transfer their sovereign defence rights to the newly-created European structure in 1992. The Maastricht Treaty also emphasised the specific character of security and defence policies of certain Member States and respected the obligations of certain Member States under NATO. Article J.4(5) gave two or more Member States legal basis for closer bilateral cooperation, in the framework of WEU or Atlantic Alliance.

Elevating defence policies to the EU level requires regulating the relationship of Member States with the WEU. Therefore, the Maastricht Treaty attempted to revitalise the WEU by recognising it as 'an integral part of the development of the Union' (Article J.4(2) TEU). However, the Maastricht Treaty did not provide for any institutional link between the EU and WEU, although it did grant the EU the competence to request that the WEU develop and implement EU decisions and undertakings with defence implications. Accordingly, the WEU Council and Council could work out "the necessary practical arrangements".

It is worth noting that some EC/EU Member States attached two declarations to TEU regarding the relationship between the EU and WEU. The first declaration (by Belgium, Germany, Spain, France, Italy, Luxembourg, the Netherlands, Portugal, and the United Kingdom of Great Britain and Northern Ireland) emphasised that WEU would become an integral part of the development process of the EU and strengthen its contribution to solidarity within NATO. The WEU should be developed as a defence component of the EU and as a means of strengthening the European pillar of NATO. Therefore, the WEU should define a common European defence policy and

practically implement it by further developing its operational role. Therefore, EU Member States and the WEU agreed to provide a new developmental impetus to the WEU, in which the WEU would be part of EU's defence. The Member States also said they would prepare the WEU to develop and implement EU decisions and actions relevant to defence at EU's request.

The second declaration (accomplished by Belgium, Germany, Spain, France, Italy, Luxembourg, the Netherlands, Portugal, and the United Kingdom of Great Britain and Northern Ireland) encouraged all EU Member States to join the WEU or obtain observer status.

Following the arrangements of the Maastricht Treaty, the WEU Ministerial Council at its Bonn session on 19 June 1992 adopted a declaration establishing the so-called Petersberg Missions.[24] These covered the conduct of the following military operations outside the territory of Member States by WEU Member States' military units operating under WEU authority: humanitarian and rescue, peacekeeping and crisis management operations.

The establishment of Petersberg Missions was linked to the building of WEU's operational capabilities, establishment of a European nuclear deterrent, development of the arms regime, and commitment to arms control and the disarmament process. Therefore, the Petersberg Declaration stipulated that military units capable of conducting Petersberg Missions should be drawn from the armed forces of WEU Member States, including those serving in NATO missions, and organised on a multinational basis. The Petersberg Declaration also contained a general commitment to develop and use appropriate capabilities to enable the deployment of WEU military units on land, sea or air for Petersberg Missions.

A tangible result of the Petersberg Declaration was the establishment of a Planning Cell within the WEU structures responsible for:

- preparing contingency plans for employment of forces under the auspices of WEU;
- drafting recommendations on necessary command, control and communication arrangements, including standing operating procedures for selected commands;
- maintaining an updated list of units that can be allocated to WEU for specific operations.[25]

However, the WEU's linkage with the EU and the adoption of the Petersberg Declaration did not lead to the revitalisation of the WEU or an increase in the EU's standing on the international stage. The only such moment occurred between 1992 and 1995 when the WEU conducted an operation in the Adriatic Sea to oversee compliance with the arms embargo and economic sanctions against Yugoslavia.

24 Western European Union Council of Ministers, 1992.
25 Ibid.

2.4. CFSP reforms introduced by the Amsterdam and Nice Treaties

The convening of another intergovernmental conference in March 1996 in Turin was motivated by the need to promote European Community/EU's actions in international relations.[26] Its aim was to revise the Maastricht Treaty, inter alia in the field of CFSP and the relationship between the EC/EU and WEU. The Intergovernmental Conference lasted for more than a year until April 1997. The draft Reform Treaty was accepted by the European Council in Amsterdam in June 1997[27] and was formally signed on 2 October 1997. The Amsterdam Treaty came into force on 1 May 1999 after ratification by all Member States.[28] In accordance with the Amsterdam Treaty, CFSP was defined and implemented by the EU (Article 11.1 TEU) and not, as before, by the EU and Member States. The Treaty of Amsterdam also expanded the catalogue of EU objectives pursued under CFSP to include:

- maintaining the territorial integrity of the EU in accordance with the principles of the UN Charter.,
- maintaining international peace and security, including the protection of EU's external borders (Article 11(1) TEU).

The Treaty of Amsterdam introduced changes to the CFSP legal instruments and decision-making procedures. While maintaining existing instruments (principles and general guidelines, common positions, joint actions and systematic cooperation), it added common strategies. The common strategies were non-binding instruments for Member States adopted by the European Council on their common interests (Articles 12 and 13(2) TEU). They define the objectives, duration and means to be made available by the EU and Member States. The Amsterdam Treaty also changed the name of systematic cooperation to strengthening systematic cooperation. Contrary to the name, strengthening systematic cooperation was informal and served to coordinate activities in international organisations and intergovernmental conferences.

The Treaty of Amsterdam, while maintaining the principle of unanimity, extended qualified majority voting in CFSP matters. Common positions, joint actions and implementing decisions were adopted by a qualified majority. If a Member State opposed a particular decision on the grounds of its national interest, then the Council could, by a qualified majority, request that the matter be referred to the European Council, which acted unanimously on the matter (Article 23(2) TEU). The Amsterdam Treaty also established the principle of constructive abstention (Article 23(1)–(2) TEU), under which even if a Member State abstained, the decision was understood to be taken unanimously. The State was not obliged to implement this decision. If abstaining Member States had more than one-third of weighted votes, they could block the decision.

26 Mik, 2000, p. 69.
27 European Council, 1997.
28 *Treaty of Amsterdam*, 1997.

The Treaty of Amsterdam also introduced institutional changes in CFSP. It established the High Representative for CSFP, Secretary-General of the Council and a Planning and Early Warning Cell. The High Representative was expected to support the Presidency and Council by formulating, preparing and implementing political decisions, and conducting political dialogue with third countries (Articles 18(3) and 26 TEU).

The Treaty of Amsterdam was also significant in relation to the defence policy. First, it gave the European Council the competence to decide on principles and general guidelines in common defence matters and set common strategies in the field of CSDP.

Second, it attempted a new arrangement of relations between the EU and WEU, giving the EU the authority to commission various types of missions to WEU. According to the wording of Article 17(1) TEU at the time, the EU should promote closer institutional relations with the WEU 'with a view to integrating the WEU into the Union, if the European Council so decides'. Accordingly, the EU took over Petersberg Missions from WEU (Article 17(2) TEU): humanitarian and rescue, peacekeeping and armed crisis management missions, and their implementation was decided by the European Council (Article 17(1) TEU). The WEU, as an integral part of EU's development, provided it with access to operational capabilities for the implementation of these missions. All EU Member States, including those with observer status in the WEU, namely Austria, Sweden, Finland, Ireland and Denmark, could participate in the implementation of Petersberg Missions (Article 17(3) TEU).

Third, the Treaty of Amsterdam also created the possibility of establishing cooperation in the field of armaments among EU Member States (Article 17(1) TEU).

Despite the formal establishment of CFSP and takeover of the Petersberg Missions from the WEU, the EU did not have any military capability to conduct these missions. The milestone decision to start building the CSDP was the Saint-Malo Declaration[29] that concerned the need for European capabilities against the background of the failure of the sole European engagement in tackling the Yugoslavian war crisis through UN peacekeeping. The declaration underlined that the Union was required to have the capacity for autonomous action, backed up by credible military forces, the means to decide to use them and a readiness to do so in order to respond to international crises.[30] The next European Council (in Cologne, 3–4 June 1999) decided to – in the framework of the CFSP – build CSDP.[31] The European Council stated that the following:

29 *Joint Declaration on European Defence, Joint Declaration issued at the British–French Summit* (Saint-Malo, 4 December 1998). [Online]. Available at: https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf. (Accessed: 5 January 2024).

30 Koutrakos, 2013, pp. 18–19.

31 European Council, 1999a.

> We are now determined to launch a new step towards the construction of the EU. Towards this end, we task the General Affairs Council to prepare the conditions and measures necessary to achieve these objectives, including the definition of modalities for the inclusion of those functions of WEU, which will be necessary for the EU to fulfil its new responsibilities in the area of the Petersberg tasks. Our aim is to make the necessary decisions by the end of 2000. In that event, the WEU, as an organisation, would have completed its purpose.[32]

At the next European Council meeting in Helsinki (10–11 December 1999), the so-called European Operational Target was proclaimed,[33] which stipulated that by the end of 2003, a corps of 50–60,000 troops would be formed, capable of carrying out Petersberg Missions of at least one year's duration within 60 days. These troops include land, sea, and airforces. However, this goal was never accomplished and the EU has never achieved the capacity to conduct military operations involving armed forces of this capacity.

In this context, the Santa Maria da Feira European Council of 19–20 June decided to develop civilian and military crisis management capabilities.[34] It was completed at the Nice European Council (7–9 December 2000), when it was decided to develop political–military structures and establish a Political and Security Committee (PSC), EU Military Committee (EUMC) and EU Military Staff (EUMS).[35]

Another decision by the Laeken European Council in December 2001 was the declaration of the Union's operational capabilities.[36] European defence policy was fully activated after the creation of the European Defence Agency (EDA) by the Thessaloniki European Council in June 2003.[37]

A major problem was defining the geographical scope of the Petersberg Missions. At the EU Defence Ministers' meeting in Sintra on 28 February 2000, it was decided that a joint force would be used on a larger scale for operations in Europe and its periphery and in smaller numbers around the world.[38]

Subsequent decisions by the European Council prepared the ground for another revision of CFSP and CSDP treaties. A new Reform Treaty was signed in Nice on 26 February 2001 and, after ratification by all Member States, entered into force on 1 February 2003.[39] The Nice Treaty sanctioned the decisions of the 1999–2001 European Council. Most notably, the provision pertaining to WEU was removed from TEU. Accordingly, the ground was prepared for the dissolution of WEU. However, it

32 Ibid.
33 European Council, 1999b.
34 European Council, 2000a.
35 European Council, 2000b.
36 European Council, 2001.
37 European Council, 2003.
38 *22 Meeting of European Union Defence Ministers*, 2000.
39 *Treaty of Nice*, 2001.

was not until the Treaty was signed in Lisbon on 13 December 2007 that the EU's actions in foreign relations under the CFSP were fundamentally restructured.[40]

3. Legal bases of the CSDP

The CSDP is not explicitly separated from all the provisions governing CFSP. In light of treaty systematics, a component of CFSP is CSDP, to which a separate section is devoted within the CFSP provisions. When analysing the common provisions on CFSP issues overall (Articles 23–41 TEU) and provisions on CSDP only (Articles 42–46 TEU), it is difficult to identify regulations on CSDP alone. Security and defence issues are inextricably linked. Therefore, when analysing the legal basis of CSDP, it cannot be isolated from other provisions governing CFSP.

The current legal basis for CSDP was shaped by the 2007 Lisbon Treaty, which brought significant changes to CFSP, including abolishing the three-pillar structure of the EU. The Union became a single legal order with a legal personality under which CFSP (especially CSDP) became one of EU's policies. The Treaties unified the EU's objectives in external relations, both for all aspects of CFSP and external actions. The EU was also given new tasks in the field of defence. In addition to the so-called Petersberg Missions, the Lisbon Treaty enabled the EU to conduct missions related to military advice or post-conflict stabilisation (Article 43(1) TEU).[41] A commitment to collective self-defence in the event of armed aggression was incorporated into the treaties (Article 42(7) TEU). Therefore, the existence of WEU as a separate organisation became redundant.[42] In 2010, President of the WEU Council declared that WEU had fulfilled its historic role, and its Member States had jointly decided to terminate the modified Brussels Treaty and dissolve WEU.[43] The Agency for the Development of Defence Capabilities, Research, Acquisition and Armaments (European Defence Agency) was given a treaty basis (Article 45 TEU). The Lisbon Treaty has also enabled Member States to deepen defence integration within the framework of permanent structured cooperation (Article 46 TEU).

40 *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing European Community*, 2007.

41 Neuhold, 2013, point 34.

42 Geiger et al., 2015, p. 159.

43 *Statement of the Presidency of the Permanent Council of the WEU on behalf of the High Contracting Parties to the Modified Brussels Treaty–Belgium, France, Germany, Greece, Italy, Luxembourg, The Netherlands, Portugal, Spain and the United Kingdom*, 2010.

3.1. Characteristics of the treaty regulations in the area of CSDP

CFSP, of which CSDP is a part, is the only EU policy and activity set out in the provisions of TEU rather than TFEU. The CFSP provisions are contained in Title V of TEU ("General Provisions on the Union's External Action and Specific Provisions on the Common Foreign and Security Policy"), comprising Articles 21–46 TEU. Other external actions of EU such as the common commercial policy, development cooperation, solidarity clause in the event of a natural disaster and humanitarian aid are regulated by TFEU. Those who drafted Lisbon Treaty singled out from all the provisions of CFSP regulations concerning only CSDP, to which Articles 4246 TEU are devoted. It follows from the systematics of the Treaties that certain announced provisions contained in Articles 23–41 TEU also apply to the CSDP, as these are common to all activities carried out under CFSP and are also applicable to CSDP.

The provisions of TEU set out objectives for CSDP (Article 21). It is worth noting that these objectives are universal in nature and are uniformly defined for all EU external actions (not only for CSDP). It follows from Article 21 TEU that the EU will be guided on the international scene by the principles of 'democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity and respect for the principles of the United Nations Charter and international law'. The EU also aims to develop relationships and build partnerships with third countries and international, regional or global organisations that adhere to the aforementioned principles. The specifications of these general objectives are formulated in Article 21(2) TEU, and the common objectives of all EU external actions, not so much the CSDP, were identified. Owing to the broadly-formulated objectives of the EU's actions in the international arena, the objectives pursued under CSDP may conflict with or overlap with other external actions of the EU.[44] Article 21 TEU does not allow for a distinction between objectives that concern only the CSDP, CFSP or other EU external actions. Therefore, it is of utmost importance to ensure coherence between EU actions undertaken in different areas of external EU activity.

The separation of CFSP and CSDP from the catalogue of other EU policies and activities (including the EU's external actions) is intended to underline their distinctiveness and specificity.[45] According to Article 24(1) TEU, CFSP is subject to specific rules and procedures and is primarily implemented by intergovernmental EU institutions (European Council and the Council). TEU provisions essentially maintain the intergovernmental nature of all CFSP and provide Member States with an enhanced ability to protect their national interests.[46] The Treaties provide considerable autonomy to Member States to formulate and implement their own security and defence policy, including the formation and accession to military alliances and specific

44 Cremona, 2018, p. 15.
45 Mikos-Sitek, 2022, p. 198.
46 de Waele, 2023, p. 36.

character of the security and defence policy of Member States. The special nature of CFSP is underlined in two declarations attached to these treaties.

In line with Declaration No. 13 on CFSP, the TEU provisions do not affect the current responsibility of Member States for the formulation and conduct of their own foreign and security policy or the manner in which they are represented in third countries and international organisations. Furthermore, they do not affect the specific nature of some Member States' security and defence policies. Declaration No. 13 emphasises that the EU and its Member States will remain bound by the provisions of the UN Charter and, in particular, by the primary responsibility of the Security Council and of its Members for the maintenance of international peace and security.

CFSP Declaration No. 14 emphasises that the existing legal basis, responsibility or powers of each Member State in the formulation and conduct of its own foreign policy, national diplomatic service, relations with third countries and participation in international organisations, including its membership in the UN Security Council, will not be affected by CFSP provisions.

Therefore, there is no doubt that the core competences in security and defence policy have been reserved to Member States.[47]

3.2. Nature of EU competence in CSDP

The distinctiveness of CSDP from other EU policies and actions in the external sphere is evident at the level of the distribution of competences between the EU and its Member States.

The basis of the EU's competence is the delegation of sovereign powers of Member States to the organisation. The CJEU has repeatedly emphasised that the EC/EU acts only within the limits of its competence.[48] The principle of conferral powers is the basic principle on which the structure of EU is based; that is, the vertical division of competences between the EU and its Member States. This implies that the EU can only act within its competences and has only as much competence as has been conferred on it by Member States. The principle of conferral of competences follows from Article 5 TEU, which states that *'The limits of the Union's competences shall be determined by the principle of conferral. The exercise of these competences shall be subject to the principles of subsidiarity and proportionality'*. The second sentence of Paragraph 2 of the TEU clarifies that any competence not conferred on the Union by the Treaties remains with Member States. Therefore, the EU does not have the same competences as its Member States; in particular, it does not possess metacompetence. The EU acts only to the extent conferred on it by the Treaties. The EU's powers are, therefore not

47 Geiger et al., 2015, p. 126.

48 Judgement of the Court of Justice of 12 September 2017, *Alexios Anagnostakis v European Commission*, C-589/15 P (ECLI:EU:C:2017:663), § 97.

unlimited, but specific and require proof.[49] The EU does not have general lawmaking powers, and every piece of legislation must have a legal basis and must be adopted in accordance with a specific procedure.[50]

Against this backdrop, Declaration 18, attached to the Treaties on the Delimitation of Competences, is particularly important. According to the declaration, all competences not conferred on the Union in the Treaties belong to Member States, and competences, even those already exercised by the Union, may revert to Member States if the Union has not exercised or has decided not to exercise its competences. The Declaration also indicates that a Member State may modify the scope of the Union's competences by amending the treaties.

The Lisbon Treaty is the first in the history of European integration, which introduced into the European legal order and defines the basic concepts pertaining to the division of competences between the EU and the Member States. Article 2 TFEU distinguishes between three main categories of EU competence: exclusive competence (Paragraph 1), shared competence (Paragraph 2) and competence to carry out actions to support, coordinate or supplement the actions of Member States (Paragraph 5) by assigning specific areas of the EU's activity in Articles 3–6 TFEU. However, CFSP has not been mentioned in any of its parts, including the CSDP.[51] However, Article 2(4) TFEU states that the EU is competent to define and implement CFSP, including the progressive definition of CSDP. This competence is exercised in the manner detailed in Title V of TEU. Therefore, Article 24 TEU is fundamental to the division of competences. According to this provision, the EU's competence in relation to the CFSP covers 'all areas of foreign policy and all matters relating to the Union's security, including the progressive definition of a common defence policy that may lead to a common defence' (Paragraph 1). The provision further stipulates that the Union shall define, conduct and implement this policy within the framework of the principles and objectives of its external action and that it shall be 'based on the development of mutual political solidarity between Member States, the identification of issues of general interest and the achievement of an ever-increasing degree of convergence between Member States' actions' (Paragraph 2). For their part, Member States shall actively and unreservedly support the Union's CFSP in a spirit of loyalty and mutual solidarity and shall respect the Union's actions in this area. They shall act in concert to strengthen and develop mutual political solidarity. Therefore, they shall refrain from any action that would be contrary to the interests of the Union or may damage its effectiveness as a cohesive force in international relations (Paragraph 3).

Determining the nature of CSDP's competence is difficult. This is certainly not exclusive, as it is not indicated in the catalogue of exclusive competences contained in Article 3 TFEU.[52] Furthermore, two declarations to Treaties (Nos. 13 and 14)

49 Cremona, 2018, p. 12.
50 de Waele, 2023, p. 7.
51 Butler, 2021, p. 41.
52 Wouters et al., 2021, p. 214.

are relevant for determining the nature of CSDP's competences. According to their wording, CFSP does not affect the responsibility of Member States for the formulation and implementation of their defence policies. Combining the wording of these declarations with the wording of Article 24 TEU, it can be concluded that EU's competences in the field of CSDP are *sui generis*.[53] What distinguishes them from shared competences is that, in the field of CFSP, the principle of "occupying the field", which is the essence of shared competences, meaning the exercise of competence by the EU and regulation of an issue precludes Member States from regulating that issue to the same extent, does not operate.[54] In the field of CFSP, EU competences can be "parallel" in the sense that both the EU and Member States can take action, including the conclusion of international agreements, on the same aspects of security and defence policy.[55]

When considering the nature of EU's competences in the field of CFSP, it should be noted that the conduct of policy on public order and protection of security has been expressly reserved in the Treaties to the Exclusive Competence of Member States (Articles 4 and 72 TEU). In contrast, under CSDP, Member States are committed to progressively improving their military capabilities (Article 42(3) TEU) and having the military capacity necessary for the EU to perform missions (outside the Union) for peacekeeping, conflict prevention and strengthening international security (Article 42(1) TEU). Building this capacity is directly related to the maintenance of public order and security. However, the boundaries between the EU's CSDP competence and exclusive competence of Member States to determine their national security are blurred, and the CJEU interprets Article 72 TFEU in a manner that narrows Member States' competence.[56]

3.3. Secondary law created under CSDP

The intergovernmental nature of CSDP affects the acts of secondary legislation adopted under it.[57] The TEU has explicitly ruled out the adoption of legislative acts under CFSP, thereby excluding the adoption of regulations and directives *(a contrario* Articles 289(1) and (2) TFEU, in conjunction with Article 24(1) TEU).

In place of the classic legal acts adopted in all EU policies and activities listed in Article 288 of TFEU, the TEU introduced legal instruments specific only to CFSP, that is, general guidelines (defined by the European Council) and decisions (adopted by European Council and the Council). The nature of these acts differs from legal acts adopted under the TFEU provisions, especially when it comes to the question of

53 Cremona, 2018, pp. 6–7.
54 Eckes, 2015, p. 543.
55 Butler, 2021, p. 41.
56 Judgement of the Court of Justice of 4 December 1974, 41/74, *Yvonne van Duyn p. Home Office,* ECLI:EU:C:1974:133; judgement of the Court of Justice of 15 December 2009, C-461/05, *Commission v. Denmark,* § 53.
57 Neuhold, 2013.

whether CFSP acts have a primacy and direct effect.[58] Neither Treaties, nor the CJEU has provided a clear answer to this question. However, decisions adopted under CFSP are not addressed to individuals, but to Member States.[59]

On the institutional side, the lack of possibility of adopting legislative acts under CFSP means that supranational institutions (the European Parliament and the European Commission) were practically excluded from the law-making process.[60] In accordance with Article 24(1) TEU, the definition and implementation of CFSP has been entrusted to European Council and the Council, that is, to intergovernmental EU institutions. Practically, CFSP is implemented by the High Representative for Foreign Affairs and Security Policy, supported by the European External Action Service (EEAS) and Member States. The TEU also significantly limited the competence of the CJEU in dealing with complaints and preliminary questions related to CFSP.

The Lisbon Treaty introduced significant changes to the entire system of application of the law, including possible forms of action under CFSP. These are reflected in the current wording of Article 24 TEU, according to which the legal instruments in the area of CFSP are general guidelines and decisions. Article 25 TEU adds to this catalogue the strengthening of systematic cooperation between Member States in the conduct of their policies, while Article 37 TEU authorises the EU to conclude international agreements in the field of CFSP. With the Lisbon Treaty entering into force, these legal instruments have replaced joint strategies, actions and positions.

None of the acts referred to in Article 24 TEU are legislative.[61] This means that the decisions of the European Council and Council are always non-legislative.

In accordance with Article 26 TEU, general guidelines are adopted by the European Council and concern not only foreign policy matters, but also issues with defence implications. The general guidelines are the basis for the development of CFSP and CSDP by the Council and the basis for decision-making. General guidelines are most often included in the conclusions of European Council summits and play a vital role in politics.

The legal instrument of primary importance for CFSP is a decision issued by the Council or European Council. Decisions may particularly concern defence issues (Article 42(4) TEU). Article 25 TEU lists three types of decisions: those that determine actions to be conducted by the EU, those that determine positions to be taken by the EU and those of an executive nature.

Decisions defining actions to be carried out by the Union are adopted by the Council, inter alia, when the international situation indicates the need to take certain operational actions (Article 28(1) TEU). These decisions make it possible to define the purpose, scope and necessary measures, and may also concern the

58 Wouters et al., 2021, p. 221.
59 Marquardt, 2018, p. 29.
60 Ibid., p. 215.
61 Geiger et al., 2015, p. 126.

allocation of financial resources for the activities to be carried out. These decisions are reminiscent of former Joint Actions and are key instruments of CFSP and CSDP in launching civilian and military operations and missions. In accordance with Article 28(2) TEU, these decisions are binding on Member States in relation to the positions they take and the activities they conduct, and Member States are obliged to ensure that their national policies are consistent with the EU position.[62] Only Member States that formally declared that they wanted to make use of a "constructive abstention" are not obliged to execute the decision.[63]

Decisions on the position to be taken by the EU follow so-called Common Positions and either concern how to deal with a particular crisis or describe the position to be taken by Member States in negotiations within international organisations.[64] These decisions, in accordance with Article 29 TEU, may define the Union's approach to a given problem from a geographical or subject-matter perspective.

Finally, the third category of decisions is executive, in that it refers to the implementation of the two previous categories of decisions.

Essentially, distinguishing between the first and second types of decisions is extremely difficult. In its judgement of 27 July 2022 (T-125/22), the General Court pointed to three elements characterising the decisions indicated in Article 29 TEU; the decision falls within the framework of CFSP, addresses 'a problem of a geographical or thematic nature' and is not of an "operational nature" within the meaning of Article 28 TEU (actions of a civilian or military nature carried out by one or more Member States outside the territory of the Union).[65] These decisions therefore include not only acts of a programmatic nature or declarations of intent, but also decisions providing for measures that may directly alter the legal situation of individuals (§ 51).

The EU also makes decisions when it establishes military and civilian missions (Article 42(4) TEU) and when it undertakes joint disarmament operations, humanitarian and rescue tasks, conflict prevention and post-conflict stabilisation measures (Article 43(2) TEU). Determining the relationship between Articles 42(4), 43(2), and 28 TEU is extremely difficult, primarily because of the lack of uniform council practice. It should be postulated that the legal bases for the adoption of decisions under Articles 42(4) and 43(2) TEU are *lex specialis* vis-à-vis Articles 28 and 29 TEU, all the more because decisions based on Articles 42(4) and 43(2) TEU are always adopted unanimously.

Decisions listed in Article 25 TEU are covered by the principle of the primacy of EU law, so that commitments entered into by Member States in the sphere of its own foreign and security policy cannot constitute grounds for non-application of

62 Geiger et al., 2015, p. 134.
63 Ibid.
64 Mikos-Sitek, 2022, p. 206.
65 Judgement of the General Court (Grand Chamber) of 27 July 2022, T125/22, *RT France v Council of the European Union*, ECLI:EU:T:2022:483, § 50.

decisions adopted by the EU in the field of CFSP.[66] This takes on a particular context in relation to membership of the UN and obligations under the UN Charter.

3.4. International agreements in the field of CSDP

According to Article 37 TEU, the EU is competent to conclude agreements with one or more States or international organisations in the CSDP field. The EU's competence to conclude international agreements is, in principle, limited because, as an international organisation, it has only the power to conclude treaties that have been delegated to it by its Member States. Such agreements may vary in nature depending on whether they relate exclusively or mainly to CSDP.[67]

Treaties do not define what an international agreement is. One of the first cases in which the CJEU addressed the problem of defining an international agreement was European Parliament and *European Commission v Council* (C-103/12)[68]. This case concerned the nature of a declaration issued by the Council and addressed to the Bolivarian Republic of Venezuela. The subject of the declaration was the granting of fishing opportunities in the exclusive economic zone, off the coast of Guyana, to fishing vessels carrying Bolivarian Republic of Venezuela flags. In its judgement of 26 November 2014, the CJEU noted that the term international agreement must be understood in a general sense, as any commitment entered into by the subjects of international law and having the force of law, regardless of its formal qualification (§ 83). The CJEU also highlighted several elements that determine the existence of an international agreement:

- the expression of consensual will of at least two States; in this particular case, it was the conclusion of an agreement through an exchange of documents; the CJEU considered the Council's declaration to be an offer by the Union to the Bolivarian Republic of Venezuela with a view to concluding an international agreement; when the declaration in question was presented to the Bolivarian Republic of Venezuela, that State acknowledged its receipt and agreed to the terms proposed by the EU;
- the agreement contains mutual rights and obligations;
- under international law, it is not important to determine whether such an agreement is embodied in one, two or more documents.

In the aforementioned case, the CJEU did not explicitly refer to the Vienna Convention of 21 March 1986 on the Law of Treaties between States and International Organisations or between International Organisations,[69] although it applied

66 de Waele, 2023, p. 57.

67 Geradin, 2015.

68 Judgement of the Court of Justice (Grand Chamber) of 26 November 2014, C103/12 and C165/12, *European Parliament and European Commission v Council*, ECLI:EU:C:2014:2400.

69 *Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations,* 1986.

the criteria for the qualification of an international agreement derived from this Convention. Formally, this Convention has not entered into force, and the EU is not bound by it.[70]

International agreements within the CSDP framework are concluded in accordance with the procedures described in Article 218 TFEU.[71] This provision sets out a uniform procedure of general scope concerning the negotiation and conclusion of such agreements, except where treaties provide for special procedures.[72] Considering its general nature, the procedure for the conclusion of international agreements must consider the specificities defined by the treaties for each sphere of action of the Union, particularly with regard to competences of institutions.[73] Therefore, establishing symmetry is intended to mirror externally the distribution of powers between the institutions applied internally, in particular, to ensure that the Parliament and Council have the same powers in the area concerned, while respecting the institutional balance defined by the Treaties.[74] The conclusion of international agreements related to CSDP is not subject to a separately regulated procedure. However, Article 218 TFEU provides for several departures from the standard procedure for the conclusion of such agreements,[75] considering the specificities of this policy. First, the position of the High Representative was strengthened, with the power to make recommendations to the Council to enter into negotiations and the power to conduct negotiations (Article 218(3) TFEU). Second, when concluding international agreements, the Council acts unanimously without the European Parliament's participation (Articles 218(6) and (8) TFEU). Nevertheless, it is obligatory to keep the European Parliament fully informed at all stages of the procedure for the conclusion of such an agreement.[76]

Pursuant to Article 216(2) TFEU, international agreements concluded by the EU in the field of CSDP are binding on the institutions of the EU and its Member States. This provision also applies to international agreements within the CSDP.[77] This means that as soon as such an agreement comes into force, its provisions form an integral part of the Union's legal order. Therefore, such agreements take precedence over legal acts issued by institutions.

70 As at 31 January 2024; data for: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXIII-3&chapter=23&clang=_en (Accessed: 5 January 2024).
71 Geiger et al., 2015, p. 145.
72 Judgement of the Court of Justice of 4 September 2018, C-244/17, *European Commission v Council*, EU:C:2018:662, § 21.
73 Judgement of the Court of Justice of 24 June 2014, C-658/11, ECLI:EU:C:2014:2025, § 53.
74 Ibid., § 22.
75 Judgement of the Court of Justice of 24 June 2014, C-658/11, *European Parliament v Council*, EU:C:2014:2025, §§ 52, 72.
76 Judgement of the Court of Justice (Grand Chamber) of 14 June 2016, C-263/14, *European Parliament v Council,* ECLI:EU:C:2016:435, § 68.
77 Butler, 2021, p. 63.

4. Decision-making mechanism in CSDP

The decision-making process under CSDP shows far-reaching distinctiveness. The exclusion of the possibility of adopting legislative acts means that the CSDP legislative competence of the two supranational institutions (the European Parliament and the European Commission) has been significantly reduced, and intergovernmental institutions, namely the European Council and Council, participate in the legislative process. Under Article 31 TEU, CFSP decisions are taken by the European Council and the Council as a rule by unanimity. This interpretation is supported by Article 42(4) TEU, according to which 'decisions relating to the common security and defence policy, including those initiating a mission as referred to in this Article, shall be adopted by the Council acting unanimously […]'.

Exceptionally, when required by a specific treaty provision, decisions may be made by a qualified majority of votes, in accordance with the general principles set out in Article 16(4) TEU. As a general rule, a qualified majority is, therefore, a so-called double majority, that is, at least 55% of Member States (but no less than 15) whose combined population makes up at least 65% of the Union's population. However, when the Council does not act on a proposal from the Commission or the High Representative of the Union for Foreign Affairs and Security Policy, a qualified majority shall be defined as at least 72% of Council members representing Member States, comprising at least 65% of the Union's population (Article 238(2) TEU). The exception described in Article 238(2) TFEU is relevant to CFSP insofar as the right of initiative for the adoption of a legislative act is also conferred on Member States or the High Representative of the Union for Foreign Affairs and Security Policy. Whenever Member States propose the adoption of a legal act, the rules for determining the qualified majority, as described in Article 238(2) TEU, will apply.

In the case of CFSP, majority voting occurs only in situations specified in the Treaties. Currently, according to Article 31(2) TEU, majority voting occurs in the council in four cases. However, if a proposed decision has military or defence implications, it must always be taken unanimously (Article 31(4) TEU). This means that the principle of unanimity will always apply to decisions made by the Council regarding CSDP. When the European Council makes a decision, it must achieve unanimity in all situations.

Unanimity means that, *de facto* each Member State has veto rights. The weakening of the veto right is the institution of constructive abstention, which was introduced in Article 31 TEU. This institution also applies to decisions adopted in the CSDP framework based on Articles 42(4) and 43(2) TEU. This is prejudiced by the wording of Article 31(1) TEU, according to which the decision-making procedure (and therefore constructive abstention) applies to all decisions adopted under CFSP and, therefore, also to decisions adopted under specific provisions governing CSDP.

The institution of constructive abstention is that any member of the Council who abstains may simultaneously make a formal declaration. By making such a declaration, the effect is that the submitting Member State is not obliged to implement the

decision, but accepts that the decision binds the Union and, in a spirit of mutual solidarity, must refrain from any action that would conflict with or impede EU action. In return, the TEU has an obligation to respect the position of Member States and make such a declaration. However, a decision cannot be made if such declarations are made by at least one-third of the Council's members, representing at least one-third of the EU population. Under these circumstances, the decision is not adopted. The population of Member States making the declaration is determined according to the same rules as those for qualified majority voting and is set out in an annex to the Council's Rules of Procedure.

An important feature of CSDP is its solutions to legislative initiatives. In principle, under EU law, such an initiative is vested in the European Commission (Article 17(2) TEU). However, the exclusion of the adoption of legislative acts in CFSP and subjection of this policy to specific rules and procedures also influenced the lawmaking process. The TEU excluded the European Commission's power of direct legislative initiative and conferred the right of legislative initiative on any Member State or the High Representative of the Union for Foreign Affairs and Security Policy (Article 30(1) TEU). Such an interpretation is reinforced by the wording of Article 42(4) TEU, which entrusts the initiative to adopt CSDP decisions to the High Representative or an EU Member State. The TEU only empowered the European Commission to "assist" the High Representative in exercising the power of legislative initiative.

5. CSDP and the sovereignty of EU Member States

European integration in the defence sphere is not without its impact on the autonomy of EU Member States in the internal and external spheres, that is, on the principle of state sovereignty. Despite this, the Treaties contain no provisions explicitly referring to the sovereignty of EU Member States. Article 4 TEU is one of the few provisions that does not explicitly address the issue of sovereignty. This provision does not use the term state sovereignty. In Paragraph 1, this provision emphasises that all competences not conferred on the Union by the Treaties belong to Member States. In contrast, Paragraph 2 of the Treaty emphasises respect for the equality of Member States before the Treaties, their national identities (including their fundamental political and constitutional structures) and respect for the essential functions of the State. According to the Treaties, the Union respects the functions designed to ensure its territorial integrity, maintain public order and protect national security. The TEU emphasises that national security remains the exclusive responsibility of individual Member States.

While there is no mention of the sovereignty of Member States in any provision of the Treaties, it refers to the principle of State sovereignty when they indicate the objectives of the EU's external action vis-à-vis third countries and international

organisations. However, they do not do so explicitly, but by general reference to the principles of the UN Charter and international law. Therefore, the objective of the EU in its external relations is to contribute to the strict observance and development of international law, particularly the principles of the UN Charter (Article 3(5) TEU). The EU's action on the international scene is based, inter alia, on the principles of the UN Charter and international law (Article 21(1) TEU). Undoubtedly, a fundamental principle of international order is the sovereign equality of states, which is the source of other principles of international law.[78] The principle of sovereign equality of States is explicitly indicated in Article 2, Paragraph 1 of the UN Charter and General Assembly Resolution 2625(XXV) of 24 October 1970 – Declaration of Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the UN Charter.[79]

The process of democratisation of state systems and formation of the nation as the subject (rather than the object) of power led to the formation of a modern understanding of sovereignty, where the sovereign is not the ruler (monarch) but the nation. Initially, it was generally accepted that the sovereign enjoyed supreme and unlimited power within national territory, both in internal relations of the state and external relations.[80] However, the institutionalisation of the international community, as reflected in the development of integration processes and increased interdependence of states, has altered this perception of sovereignty. The doctrine of international law reflects the notion that absolute unlimited sovereignty is something of the past.[81] International law literature views sovereignty as meta-sovereignty, that is, competence to ultimately decide whether and how to exercise particular attributes and functions of a state.[82] Attributes of sovereignty so understood include, exclusive jurisdictional competence over individual territories and citizens; exercise of foreign policy powers; deciding on war and peace; freedom in the recognition of states and governments; establishing diplomatic relations; deciding on military alliances and membership in international political organisations; and conducting independent financial, budgetary and fiscal policies.

Understood in this way, sovereignty is an intrinsic feature of a state that distinguishes it from other subjects of international law (including inclusive international organisations). If a state loses its ability to exercise meta-sovereignty, it forfeits its sovereignty and ceases to exist as a subject of international law. However, a consequence of this understanding of sovereignty is that a state may restrict the exercise of certain sovereignty attributes.[83] A distinction is made between restrictions on sovereignty that result from the will of the state (which is compatible with international

78 Cassese, 2001, p. 88.
79 *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, A/RES/2625(XXV), 1970.
80 Anand, 1986, p. 25.
81 Ibid., p. 27.
82 Mik, 2022, p. 436.
83 Anand, 1986, p. 34.

law) and violations of sovereignty that occur against the will of the state and are incompatible with international law.[84] Voluntary restrictions by a state on the attributes of sovereignty are generally imposed by international agreements and do not imply a loss of sovereignty or statehood. Such action does not limit (or deprive) sovereignty; rather, it is an evidence of sovereignty.[85] The ability of a state to enter international obligations is inherent in its legal nature and constitutes its identity in international law.[86]

The discussion on the importance of sovereignty in the process of European integration has been ongoing since the beginning of Communities/Union and intensified in the 1990s, after European integration was extended to the political–military fields. In particular, following the 2007 Lisbon Treaty reform, the CFSP encompasses all areas of foreign policy and issues relating to the Union's security, including the progressive definition of CSDP, which may lead to a common defence (Article 24(1) TEU). Therefore, CFSP, especially CSDP, encompasses activities that are traditionally part of the attributes of sovereignty and are conducted by States. This includes, in particular, the exercise of foreign-policy competences, establishment and maintenance of diplomatic relations, maintenance of armies and deciding on political–military alliances. These areas are partly covered by the process of European integration, but CFSP and CSDP have maintained their far-reaching autonomous character within the EU legal order.

However, the process of transferring competencies from the Member State-level to the EU has neither led to a loss of sovereignty for EU Member States nor a permanent reduction in the sovereign rights of Member States.[87] The process of political–military integration is irreversible. Although dynamic in nature, Member States retain meta-competence and are entitled to decide the pace and degree of European integration.[88] The decision to deepen integration, including into the political and defence spheres, is reserved exclusively for Member States and can only be taken through an amendments to existing Treaties. Against this background, the simplified procedure for amending TEU, as described in Article 48(7) TEU, does not concern the extension of EU's competences in the field of CFSP or the voting system in the European Council. Nor can the simplified procedure for amending the TEU concern the mode of decision-making by the council affecting military or defence matters. Possible amendments to TEU concerning these matters can only be made in an international agreement amending existing treaties.

Treaties contain several other arrangements that safeguard the sovereignty of Member States in the field of integration in defence matters.[89] First, the treaties preserve unanimity in determining the policy directions and priorities of the CFSP, as

84 Muszyński, 2011, p. 178.
85 Permanent Court of International Justice, *S.S. "Wimbledon"* Case, Serie A, no. 1, p. 25.
86 Kwiecień, 2004, p. 128.
87 Judgement of the Polish Constitutional Court of 24 November 2010, OTK ZU 9A/2010, item 108.
88 Mik, 2022, pp. 437–438.
89 Muszyński, 2011, p. 179.

well as in many legally binding decisions (Article 31 TEU). Wherever treaties require unanimity, the lodging of a veto by a Member State prevents EU institutions from making a decision. According to the Treaties, an EU Member State may also veto any decision taken by a qualified majority if compelling reasons of national policy so warrant (Article 31(2) TEU). In such a case, a vote does not take place, and Member States should find a solution that satisfies not only the majority of states but, above all, the State issuing the veto.

Safeguarding the sovereignty of States in the process of politico–defence integration also emphasises the primary responsibility of Member States for the formulation and conduct of their own foreign policy, the formation of their national diplomatic service and shaping of their relations with third countries, their participation in international organisations, and for the exercise of the active right of legation to ensure the representation of those Member States in third countries and international organisations (Declaration Nos. 13 and 14 of the Treaties). The Treaties also emphasise that the establishment and operation of CFSP may not affect the specific character of the security and defence policies of certain Member States (Article 42(2), TEU).

An expression of State sovereignty is the possibility of withdrawing from the EU, as stated in Article 50 TEU. The transfer of competencies from the level of a Member State to the EU is therefore not irreversible, and a Member State may withdraw from the EU the attributes of sovereignty previously transferred to it. The guaranteed nature of Article 50 TEU was also highlighted by the CJEU in its preliminary ruling of 10 December 2018 in Case C-621/18.[90] The CJEU emphasised that the purpose of Article 50 TEU is to recognise the sovereign right of a Member State to withdraw from the Union (§§ 56–57). It is a unilateral decision by that State not dependent on the consent of other Member States or the EU institutions (§ 72). The decision to withdraw is subject to the sole will of that Member State, respecting its constitutional requirements, and consequently depends on its sole sovereign choice (§ 58). Nor is the decision to withdraw from the EU conditional on the negotiation of a withdrawal agreement that sets the framework for the future relationship between the EU and such a State. While the negotiation of such an agreement is conducive to structuring the process of a Member State's withdrawal from the EU, past practice has shown that such negotiations are extremely difficult and complicated.

The mechanism protecting the sovereignty of EU Member States is the aforementioned obligation to respect the national identities inherent in their basic political and constitutional structures. Article 4 TEU formulates certain non-transferable attributes of sovereignty from the level of Member States to the level of the EU, which relate to the exercise of core functions of the State, notably to ensure its territorial integrity, maintain public order and protect national security. Article 4(2) TEU formulates only an exemplary catalogue of such non-transferable state functions, but

90 Judgement of the Court of Justice of 10 December 2018, C-621/18, *Andy Wightman and Others v Secretary of State for Exiting the European Union*, ECLI:EU:C:2018:999.

this undoubtedly includes the prohibition on the transfer of powers to create competences. The prohibition on the transfer of competencies to the EU level is particularly relevant in view of the CJEU's repeated emphasis that the process of European integration (and thus, the transfer of state attributes and functions to the EU level) is not yet complete.[91]

6. The institutional structure of the CSDP

The CSDP is managed by several EU institutions, bodies, and agencies. Of primary importance are institutions of an intergovernmental nature (the European Council and Council), while the importance of supranational institutions (above all, the European Commission and European Parliament) is limited.[92] Meanwhile, the role of CJEU requires a separate discussion. In the CSDP, there are dedicated bodies established by TEU (including the High Representative for Foreign Affairs and Security Policy and the Political Committee) and numerous *sui generis* bodies (bodies established under secondary law), whose competences are limited exclusively to CSDP.

6.1. Importance of EU institutions in the field of CSDP

Of the seven EU institutions listed in Article 13(1) TEU, the European Council and Council have the most significant influence on CSDP. Their competences in this area are set out under Article 26 TEU.

The task of the European Council is to set general orientations for foreign and security policies and to define the interests of the EU (Article 26 TEU). The European Council may introduce common defence if it decides unanimously (Article 42(2) TEU). In the framework of the European Council or the Council, all Member States must consult each other before making any decision or commitment affecting the interests of the Union (Article 32 TEU). The European Council may then define a common EU approach on a particular matter. It is also responsible for electing the President of the European Council, who manages the work of the European Council, represents the Union externally, and convenes meetings of the European Council

91 In Opinion 2/13 of 18 December 2014. The CJEU noted that '[…] the founding Treaties, which constitute the Union's basic constitutional charter […], have, unlike ordinary international agreements, established a new legal order with its own institutions, in favour of which States are increasingly restricting their sovereign rights and whose subjects are not only Member States but also individuals from them'. Similarly, Opinion of the Court of Justice 1/09 of 8 March 2011, ECLI:EU:C:2011:123, § 65 and Judgement of the Court of Justice of 10 December 2018, C-621/18, *Andy Wightman and Others v Secretary of State for Exiting the European Union,* ECLI:EU:C:2018:999, § 44.

92 Eckes, 2015, p. 539.

when international developments require the definition of lines of action for the EU (Article 15(5) TEU).

The European Council is also competent in appointing the High Representative of the Union for Foreign Affairs and Security Policy; it may also terminate his/her terms of office (Article 18(1)).

Should the need arise, the President of the European Council may convene an extraordinary meeting in order to define the strategic lines of the Union's policy in the wake of such a situation (Article 26(1) TEU).

The Council, in terms of the CSDP, has policy setting and coordination functions. Its key CSDP functions include:

- developing CSDP (Article 26(2) TEU),
- making decisions necessary to define and implement this policy (Article 26(2) TEU),
- ensuring unity, consistency and effectiveness of EU action (together with the High Representative; Article 26(2) TEU)),
- enabling the exchange of views and information between Member States,
- authorising the opening of negotiations, issuing negotiating directives and authorising the signing and conclusion of agreements (Article 218(2) TFEU).

The CSDP (and in general, CFSP) is the only area in which the European Commission does not exercise day-to-day policy and legislative functions, and its competences are significantly limited. The President of the European Commission is a member of the European Council; if the agenda so requires, he/she may be accompanied by another member of the Commission (Article 15(2) TEU). One of its vice presidents is the EU High Representative (Article 18(4), TEU).

As part of its CSDP tasks and competences, the European Commission:

- ensures consistency of different areas of the Union's external action (together with the Council and assisted by the High Representative, Article 21(3) TEU),
- may request an opinion from the CJEU on the compatibility of the envisaged international agreement with treaties (Article 218(11) TFEU),
- supervises relations with the organs of the United Nations and its specialised organisations, the Council of Europe, the Organisation for Security and Co-operation in Europe, the Organisation for Economic Cooperation and Development and other international organisations (Article 220 TFEU),
- may, together with the High Representative for Foreign Affairs and Security Policy, address any questions to the Council related to the CFSP and CSDP,
- may, where appropriate, propose the use of both national means and union instruments with the High Representative when deciding to undertake peacekeeping, conflict prevention and international security enhancement missions.

The European Parliament's role under CFSP also remains limited. As the adoption of legislative acts is excluded under the CFSP, the European Parliament does not

perform its main function (the legislative function). The European Parliament primarily has control and advisory functions (Article 36 TEU):

- is regularly consulted and informed by the High Representative of developments in the CFSP and CSDP,
- holds a debate twice a year on the progress in implementing the CFSP, including the CSDP.
- the High Representative must consider this view when deciding on foreign and security policy,
- may ask questions of the Council and the High Representative or make recommendations regarding CFSP, including CSDP.

6.2. Competence of the Court of Justice of EU in the area of CSDP

The CJEU's competence in the field of CSDP has been significantly limited. Pursuant to Article 24(1) TEU, the CJEU has no jurisdiction over these provisions, except for its jurisdiction to review compliance with Article 40 TEU and the legality of certain decisions provided for in Article 275(2) TEU. This means that the CJEU's jurisdiction is almost entirely excluded from this area, so the legal instruments adopted under the CSDP are practically beyond judicial control.[93] Article 24(1) TEU and Paragraph 1, Article 275 TFEU must be interpreted restrictively.[94] Therefore, it cannot interpret primary law in this field by way of a preliminary ruling, nor can it review the legality of CSDP decisions. However, the case law of CJEU emphasises that the CJEU has the jurisdiction to give a preliminary ruling under Article 267 TFEU on the validity of an act adopted on the basis of CSDP legislation, provided that the request for a preliminary ruling concerns either a review of the compatibility of that decision with Article 40 TEU or a review of the legality of restrictive measures adopted against natural or legal persons (Article 275 TFEU).[95] However, the CJEU's competence to give preliminary rulings on the interpretation of laws created in the CSDP appears to be excluded. Also excluded is a proceeding against a Member State under Article 258 TFEU with a complaint of failure to comply with CSDP obligations under TEU.[96]

However, the current treaties provide for the CJEU's competence to rule on CSDP matters in two situations, as set out in Articles 40 TEU and 275 TFEU.

First, the CJEU has jurisdiction to monitor compliance with Article 40 TEU. Under this, the implementation of all issues belonging to CFSP (also CSDP) is without prejudice to the application of the procedures and powers of the institutions provided

93 Judgement of the Court of Justice of 24 June 2014, C-658/11, *European Parliament v Council*, EU:C:2014:2025, § 69; Judgement of the Court of Justice of 6 October 2020, C-134/19 P, *Bank Refah Kargaran,* ECLI:EU:C:2020:793, § 26.

94 Judgement of the Court of Justice of 6 October 2020, C-134/19 P, *Bank Refah Kargaran,* ECLI:EU:C:2020:793, § 32.

95 Judgement of the Court of Justice of 28 March 2017, C-72/15, *Rosneft,* ECLI:EU:C:2017:236, § 81.

96 Contartese, 2017, p. 1630.

for in the treaties for the exercise of EU competence. Conversely, the implementation of EU policies is without prejudice to the application of the procedures and powers of the institutions provided for in the Treaties for exercising the EU's CFSP competences.

Under this jurisdiction, the CJEU acts as the "guardian of the borders" between the CSDP and other EU policies and actions (in particular the so-called "external actions of the Union" set out in Articles 206-216 TFEU).[97] Article 40 TEU statutes distinguishes the two regimes: the ordinary EU regime (EU policies and actions of a supranational nature, including external actions such as humanitarian aid) and CSDP (and other aspects of CFSP).[98] Article 40 TEU emphasises that the Union's competences under CSDP and under other provisions of the TFEU relating to Union policies and actions are not mutually exclusive but complementary, each with its own scope of application and pursuing different objectives.[99]

Under Article 40 TEU, the CJEU has no general competence to assess the legality of acts adopted under CSDP, and the only issue it may consider is the inappropriateness of the legal basis, that is, that the act should have been adopted under procedures applicable to Union policies and activities other than the CSDP.[100] This implies that an action alleging infringement of Article 40 TEU may be brought under Article 263 TFEU by the three categories of entities specified in that provision (including, inter alia, natural or legal persons). The CJEU has emphasised on several occasions that, based on Article 40 TEU, it is obliged to ensure that decisions adopted in the field of the CFSP do not encroach on the competences which the provisions of TFEU confer on the EU in the field of policies other than CFSP.[101]

Second, CJEU has the competence to review the legality of decisions that provide restrictive measures against natural or legal persons as adopted by the Council (Article 275(2) TFEU). It should be emphasised that the right of individuals to bring direct actions against decisions providing for restrictive measures against them is a *novelty* introduced by the Lisbon Treaty. Interestingly, the CJEU has developed jurisprudence whereby Article 24(1) TEU refers to Article 275(2) TFEU not to define the type of procedure by which the Court may review the legality of certain decisions but to define the type of decisions whose legality may be reviewed by the Court in the context of any procedure for such review of legality.[102] To clarify, the review of the legality of decisions of the Union takes place under two complementary procedures set out in Article 263 TFEU (the so-called action for annulment) and Article

97 Schmidt, 2020, p. 282; Eckes, 2016, p. 500.

98 Geiger et al., 2015, p. 149.

99 Judgement of the Court of Justice of 19 July 2012, C-130/10, *European Parliament v Council*, EU:C:2012:472, § 66.

100 Hillion and Wessel, 2018, pp. 71–72.

101 Judgement of the Court of Justice of 19 July 2012, C-130/10, *European Parliament v Council*, EU:C:2012:472, § 66 et seq.; Judgment of the General Court of 27 July 2022, T-125/22, *RT France v Council*, §§ 6-64.

102 Judgement of the Court of Justice of 28 March 2017, C-72/15, *Rosneft,* ECLI:EU:C:2017:236, § 70.

267 TFEU (the question for a preliminary ruling). Both procedures establish a complete system of legal remedies and procedures to ensure the review of the legality of Union acts, entrusting them to Union Courts.[103] Inherent in that complete system of legal remedies and procedures is the right of individuals to challenge the legality of Union acts either by bringing an action under Article 263 TFEU or by raising a plea for their invalidity before a national court and having the national court, which has no jurisdiction to declare such invalidity itself, submit a question to the Court of Justice for a preliminary ruling in that regard.[104] Interpreting Article 275(2) TFEU narrowly and excluding the possibility for the courts of Member States to refer for a review to the CJEU the validity of a Council decision taken in the field of CFSP would be, according to the CJEU, contrary to the structure of the system of effective judicial protection established by the treaties.[105]

The recent jurisprudence of the CJEU extends the scope of application of Article 275(2) TFEU to actions containing a claim for compensation for damage and harm allegedly suffered by the applicant as a result of the restrictive measures provided against him in the decision based on Articles 25 and 29 TEU.[106] Article 275 TFEU does not expressly mention the jurisdiction of CJEU to rule on the damage and harm allegedly suffered owing to the restrictive measures provided for in CFSP decisions.[107] Since the CJEU has jurisdiction to rule on actions for damages and compensation insofar as they relate to restrictive measures provided for in regulations made pursuant to Article 215 TFEU, the necessary coherence of the system of judicial protection under Union law requires that, in order to avoid a gap in the judicial protection of natural or legal persons affected by restrictive measures, the Court of Justice of the EU should also have jurisdiction to rule on the damages and harm allegedly suffered by reason of the restrictive measures provided for in CFSP decisions.[108]

CJEU's jurisdiction concerns decisions adopted by the Council. Therefore, neither does it cover the acts of the European Council, nor are all Council decisions subject to CJEU review, except those that 'provide for restrictive measures against natural or legal persons'. Article 275 TFEU primarily concerns decisions imposing "smart sanctions", consisting, inter alia, of freezing the funds of persons linked to terrorists. The application of such sanctions typically occurs in two stages. First, a unanimous CFSP decision of the Council providing for the possibility of imposing restrictive measures is taken. This is implemented by the Council, which, based on the basis of Article 215 TFEU, issues the necessary acts imposing restrictive measures against natural or legal persons. In doing so, the Council acts by a qualified majority on a joint proposal

103 Judgement of the Court of Justice of 25 June 2020, C-14/19 P, *European Union Satellite Centre,* ECLI:EU:C:2020:492, § 60.
104 Ibid., § 67.
105 Ibid., § 76.
106 Judgement of the Court of Justice of 6 October 2020, C-134/19 P, *Bank Refah Kargaran,* ECLI:EU:C:2020:793.
107 Ibid., § 31.
108 Ibid., §§ 37–39.

from the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission. The European Parliament shall be informed of the adoption of the act.

The procedure indicated in Article 275 TFEU for the CJEU to review Council decisions concerns those taken within the framework of the CFSP. In contrast, the measures imposing these restrictions adopted by the Council on the basis of Article 215 TFEU assume the form of an ordinary act of EU law. Therefore, they are subject to a full review by CJEU.

However, not all decisions issued under CSDP and the restrictive measures imposed can become the subject of complaints under Article 275(2) TFEU. The condition for challenging these acts before EU courts is their individual nature.[109] Therefore, if the restrictive measures provided in the decision are general, as they apply to objectively defined situations and to categories of persons and entities indicated generally, such a decision cannot be regarded as providing restrictive measures against natural or legal persons within the meaning of Article 275(2) TFEU. In this regard, it is irrelevant that the applicant challenged the provision insofar as it concerned him.

It is debatable whether the CJEU has the competence to give an opinion on the compatibility of international agreements concluded on the basis of Article 37 TEU with the Treaties.[110] According to Article 218(11) TFEU, a Member State, the European Parliament, the Council, or the Commission may obtain the opinion of the CJEU on the compatibility of an envisaged agreement with the Treaties. The competence of CJEU to provide such an opinion is, of course, not doubtful in the case of international agreements concerning external actions regulated by TFEU. This is disputable when the envisaged agreement relates exclusively or primarily to CFSP. Article 218(11) TFEU is part of the uniform procedure for the conclusion of international agreements by the EU, which also applies to CFSP, and argues in favour of giving CJEU the competence to provide an opinion on the compatibility of such an agreement with the Treaties.[111] Meanwhile, Article 218(11) TFEU also confers competence to request that the CJEU give an opinion to the European Commission and the European Parliament, which are generally excluded from the scope of CFSP. Interestingly, Article 218 TFEU does not confer any power on the High Representative. The Court has not yet had the opportunity to rule out the admissibility of issuing such opinions.

Neither Article 218 TFEU nor any provision of CFSP exclude the competence of supranational institutions to request that CJEU provide an opinion on the compatibility of an international agreement with the provisions of CSDP.[112] It must be expressed that the CJEU has the competence to give an opinion on draft international agreements, which exclusively or predominantly concern CSDP. Moreover, a request

109 Judgement of the General Court of 4 June 2014, T67/12, *Sina Bank v Council*, EU:T:2014:348, § 38.
110 Hillion and Wessel, 2009; Butler, 2021, p. 98.
111 Wouters et al., 2021, p. 217.
112 Eckes, 2016, p. 501.

for such an opinion may come from all entities identified in Article 218(11) TFEU. However, the scope of these requests remains unclear. According to the established CJEU case law, a request for an opinion may concern the substantive or formal validity of an agreement in light of the Treaty. Therefore, the CJEU's ruling on the compatibility of a proposed agreement with the Treaties may concern not only EU substantive law but also provisions concerning competence, procedures or the institutional organisation of the EU.[113] The CJEU's opinion may relate, in particular, to the division of competences between EU and Member States under CSDP.

6.3. Treaty bodies in-charge of dealing with CSDP

Bodies dealing with CSDP include the EU High Representative for Foreign Affairs and Security Policy, EEAS and PSC. The first two bodies conduct tasks not restricted to CSDP, while the PSC is a treaty body operating only in CFSP, especially CSDP.

6.3.1. EU High Representative for Foreign Affairs and Security Policy

The EU High Representative for Foreign Affairs and Security Policies has a strong influence on decisions taken in the CFSP. The High Representative is elected by the European Council by a qualified majority with the consent of the President of the European Commission (Article 18(1) TEU). However, the informal meeting of the European Council, on 19 November 2009, abandoned majority voting in favour of a consensual political agreement.

The High Representative represents the EU in the field of foreign and security policy and conducts political dialogue with third countries and other international organisations (Articles 27(1) and (2) TEU). He implements the decisions taken by the European Council and the Council in the field of CFSP (Article 27(1) TEU). However, it should be stressed that the High Representative exercises this competence jointly with Member States (Article 26(3) TEU). They may also make proposals and initiatives concerning CFSP, especially CSDP, to the Council, including a direct legislative initiative that the High Representative shall conduct alone or with the support of the European Commission (Article 30(1) TEU). He also informs the European Parliament about policy orientations in areas concerning CFSP (Article 36 TEU).

Defining the status and formal position of the High Representative within EU institutions is relatively complicated. The High Representative is closely connected to three institutions: the European Council, the Council, and the European Commission.

The status of the High Representative is not identical within intergovernmental institutions (European Council and Council). In the European Council, the High Representative participates in principle (Article 15(2) TEU). He is therefore not formally its member, and Treaties exclude him from the European Council's decision-making

113 Opinion of the Court of Justice of 30 November 2009, 1/08, ECLI:EU:C:2011:123, §§ 108–109.

powers. According to Article 15(4) TEU, as a rule, the European Council takes decisions by consensus, which is reached among its members (i.e. the President of the European Council, the Heads of State or Government of the Member States and the President of the European Commission). This aligns with the European Council's move to make decisions by vote. Therefore, the role of the High Representative in the European Council concerns participating in debates, initiating certain solutions and sharing external representation of the EU in CFSP matters with the President of the European Council. Regarding the latter, the Treaties provide that this competence is exercised by the President of the European Council without prejudice to the powers of the High Representative (Article 15(6) *in fine* TEU).

In the Council, the position of the High Representative is defined by Article 18(3) TEU. According to this provision, the High Representative chairs ex officio one of the Council configurations (i.e. the Foreign Affairs Council). The High Representative is not a member of the Council, and does not have the right to vote (Article 16(2) TEU). Giving the High Representative leadership of the Foreign Affairs Council certainly strengthens the coherence of the EU's external policies. The Foreign Affairs Council is not only responsible for CFSP, but also for other external actions of EU (such as the Common Commercial Policy and humanitarian aid).

By law, the High Representative remains one of the Vice-Presidents of the European Commission (Article 18(4) TEU). The Treaties do not attach any specific role or competence to the status of the Vice President of the European Commission. It is the President of the European Commission who is responsible for the division of responsibilities within the European Commission and determining the guidelines within which the European Commission performs its tasks as well as the internal organisation of the European Commission. Therefore, it determines how the relationship between the High Representative and other Commissioners is shaped.

6.3.2. European External Action Service

The Treaty of Lisbon established the European External Action Service (EEAS, which functions on the basis of Article 27(3) TEU and the Council Decision of 26 July 2010.[114] The seat of EEAS is Brussels (Article 1(2) of the Decision).

According to TEU, EEAS is responsible for the EU's diplomatic relations with third countries and third international organisations and conducts the EU's foreign and security policy. These tasks were further detailed in the 2010 decision and included the following:

- supporting the High Representative in the conduct of CFSP;
- cooperation with the diplomatic services of Member States;
- responsibility for diplomatic relations and promotion of strategic partnerships with non-EU countries (Article 2 of the Decision).

114 *Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service*, 2010.

The 2010 Decision contains provisions on the organisation of EEAS. The High Representative of the Union for Foreign Affairs and Security Policy (Article 1(3) of the Decision) heads the EEAS. According to Article 27 TEU, the EEAS comprises officials from the General Secretariat of the Council and the European Commission, as well as staff from national diplomatic services. The EEAS is composed of officials performing their tasks in Brussels and in EU Delegations (Article 1(3) of the Decision).

The central administration of EEAS, which performs its tasks in Brussels, is divided into directorates (Article 4 of the Decision). The Decision lists six directorates distinguished by geography (Asia and the Pacific, Africa, Europe and Central Asia, North Africa, Middle East, Arabian Peninsula, Iran and Iraq, Directorate for the Americas and Directorate for Global and Multilateral Issues) and two directorates based on theme (Directorate for Crisis Response and Operational Coordination and Directorate for Administration and Finance).

The managing directors of the directorates, together with PSC Chairman, formed the Political Council. In addition to the Policy Board, there is also a Governing Board comprising the High Representative, Secretary-General and Chief Operating Officer.

According to the 2010 Decision, the decision to open or close a delegation shall be adopted by the High Representative in agreement with the Council and the European Commission (Article 5(1)). Each delegation shall be led by a Head of Delegation who shall have authority over all staff employed in the delegation (Article 5(2)). The Head of Delegation is directly responsible for the High Representative, from whom he receives instructions and to whom he is accountable for their implementation. In specific cases, such instructions may also be provided to the Head of Delegation by the Commission.

Each Union Delegation shall be subject to periodic financial and administrative audits by the Executive Secretary-General of EEAS (Article 5(5)).

The Head of the EU Delegation was appointed by the President of the European Council and the President of the European Commission based on a proposal by the High Representative. He/she shall be selected from among candidates drawn from the EEAS, the European Commission, the European Council and the 27 Ministries of Foreign Affairs of the Member States (Article 5(6) of the Decision).

EU delegations enjoy diplomatic privileges and immunities in accordance with the provisions of the Vienna Convention on Diplomatic Relations of 18 April 1961 (Article 5 of the Decision). This is intended to ensure not only security but also full freedom of the delegation's diplomatic activity.

The tasks of the delegations are defined in Article 5 of the Council Decision:

- Facilitating contact between EU institutions and third countries or international organisations to which they are accredited;
- The Head of Delegation represents the EU as a whole in a third country or before an international organisation to which he/she is accredited, including

the power to conclude agreements and appear before courts as a party to proceedings;
- Delegations are obliged to maintain regular contact with the diplomatic missions of EU Member States and to exchange information;
- At the request of Member States, delegations support them in their tasks, including providing consular care for EU citizens.

The EU is currently represented by 140 countries and international organisations. The EU is delegated to the UN headquarters in New York, Geneva, Paris, Rome, Vienna and Nairobi, among others.

The EU Intelligence and Situation Centre (INTCEN) is an integral part of EEAS. It is the EU's civilian intelligence unit, and its tasks include providing intelligence analysis, early warning and situational awareness to the High Representative, Member States and various EU decision-making bodies. INTCEN collects information, produces its own documentation and receives data from national secret services. Central to its work is a cell composed of intelligence officers from Member States for the exchange of classified information.

INTCEN acts as a 24/7 operational focal point, monitoring and assessing international events and offering immediate facilities to support the Crisis Task Force.

6.3.3. Political and Security Committee

The Political and Security Committee (PSC), which functions on the basis of Article 38 TEU, is composed of permanent representatives of Member States and chaired by representatives of EEAS delegated by the High Representative. The PSC's tasks include:
- observing the international situation and implementing policies agreed under CFSP;
- contributing to the definition of policies by issuing opinions to the Council;
- exercising political control and the direction of crisis management operations, under the responsibility of the Council and High Representative.

The PSC is advised by the Committee on Civilian Aspects of Crisis Management (CIVCOM), which provides information, develops recommendations and presents its views on civilian aspects of crisis management to the PSC and the Political–Military Group.

6.3.4. European Defence Agency

The European Defence Agency (EDA) was established in 2004 and currently has its legal basis in Article 45 TEU, supplemented by Council Decision 2015/1835 of 12 October 2015 defining the EDA's statute, seat, and rules of operation.[115]

The Agency is under the authority of the Council and has its seat in Brussels (Article 45(1), TEU).

The Agency's tasks regulated in Article 45 TEU include:

- contributing to the definition of Member States' military capability objectives and assessment of the implementation of Member States' capability commitments;
- promoting harmonisation of operational requirements and establishing effective and consistent procurement methods;
- proposing multilateral projects to achieve military capability objectives and ensuring the coordination of programmes implemented by Member States and management of specific cooperation programmes;
- supporting defence technology research, coordinating and planning joint research activities and studying technical solutions for future operational requirements.
- contributing to the identification of any useful measures to strengthen industrial and technological base of the defence sector and enhancing the efficiency of military expenditure and, where appropriate, implementing these measures.

The 2015 Decision elucidates that the agency's mission does not prejudice the competence of Member States in defence matters (Article 2(3)).

The Agency is open to all Member States wishing to participate in its activities and is funded by the participating States. Any Member State wishing to participate in the Agency's work shall notify the Council of its intention and inform the High Representative (Article 1 of the Decision).

6.4. Organs sui generis

Sui generis bodies operate on the basis of a European Council or Council decision. They are intended to support the EU's civilian or military crisis management missions, and thus contribute to CSDP's tasks.

Military bodies include the EUMC, EUMS and Military Planning and Conduct Cell (MPCC). The structures that improve the conduct of civilian crisis management missions are Civcom and Civilian Planning and Conduct Cell.

115 *Council Decision (CFSP) 2015/1835 of 12 October 2015 defining the Statute, seat and functioning of the European Defence Agency (recast)*, 2015.

6.4.1. Military bodies

The EUMC was created and operated based on the Council Decision of 22 January 2001.[116] The decision follows the political decision taken by the Nice European Council in 2000 to strengthen CFSP and prepare the EU institutionally to conduct a full range of tasks related to the implementation of Petersberg Missions.[117]

It is the highest military body established within the Council. It is composed of the Chiefs of Defence of Member States, represented by their military representatives (Article 1 of the Decision). The EUMC's task is to provide military advice to PSC and make recommendations on all military matters within the EU. In crisis management situations, at the request of the PSC, the EUMC issues an Initial Directive to the Director General of EUMS to draw up and present strategic military options. The EUMC also assesses the strategic military options developed by the EU Military Staff and forwards them to PSC, together with its assessment and military advice. Based on the military options selected by the Council, it approves the Initial Planning Directive for the Operation Commander. It also advises PSC on options for terminating military operations.

The EUMC exercises military direction for all military activities within the EU, monitoring proper execution of military operations under the responsibility of the Operation Commander.

The EUMC is headed by a President appointed by the Council, whose term is three years.

The EU Military Staff (EUMS) was created based on the Council Decision of 22 January 2001 on the establishment of the Military Staff of the EU.[118]

The EUMS is composed of military personnel seconded by Member States. All EUMS members must be nationals of EU Member States (Articles 1 and 3 of the Decision). The EUMS works under the guidance of the EUMC, receives regular feedback and assists in all practical aspects of strategic planning (Annex to the Decision).

In 1999, the Helsinki European Council emphasised that the EUMS should provide military expertise and support to the Common European Security and Defence Policy, including the conduct of EU-led military crisis management operations. Accordingly, the tasks of the EUMS include dealing with early warnings, situation assessments and strategic planning for Petersberg Missions, together with the identification of European national and multinational forces and the implementation of policies and decisions as recommended by EUMC.[119]

The EUMS operates in the military direction of EUMC to which it reports (Annex to the Decision). The EUMS is now part of the EEAS. EUMS is directed by an Admiral.

116 *Council Decision of 22 January 2001 setting up the Military Committee of the European Union,* 2001.
117 European Council, 2000b.
118 *Council Decision of 22 January 2001 on the establishment of the Military Staff of the European Union*, 2001.
119 European Council, 1999.

During crisis management or exercises, the EUMS may establish Crisis Action Teams, drawing upon its own expertise, the state of the army and infrastructure. In addition, it may, if necessary, draw upon external forces from EU Member States for temporary reinforcement requested by the EUMC from EU Member States.

Within EUMS structures, the MPCC was created following a proposed by the Council in its conclusions of 6 March 2017[120] and the current legal basis is provided by Council Decision (EU) 2017/971 of 8 June 2017, which defines the arrangements for planning and conducting EU military CSDP missions without an executive mandate.[121]

The MPCC is based in Brussels, and is tasked with the operational planning and conduct of non-executive mandate missions, that is, non-combat missions deployed in a third country, where the EU supports the host country in an advisory role only (Article 1 of the Decision). This includes the establishment, mobilisation, sustainment and reconstitution of EU forces. The MPCC operates under the political control and strategic direction of the PSC (Article 1(3) of the Decision). The MPCC is led by the Director General of EUMS who simultaneously serves as Mission Commander for military missions without an executive mandate.

6.4.2. Civilian bodies

The structures that improve the conduct of civilian crisis management missions are Civcom and CPCC.

The CPCC is a permanent structure operating within the EEAS and is responsible for the preparation and implementation of civilian CSDP operations. The CPCC is under the political control and strategic direction of PSC and the overall authority of the High Representative.

Civcom operates on the basis of Council Decision 2000/354/CFSP of 22 May 2000 establishing a Committee on the Civilian Aspects of Crisis Management.[122] The Committee is composed of representatives of Member States and acts as a working group for the Council (Article 1).

Civcom's provides information, recommendations and advice on civilian aspects of crisis management to PSC and other relevant Council bodies, in accordance with their respective competences (Article 2). Accordingly, Civcom's tasks include:

– preparing plans for new missions;

120 European Council, 2017.

121 *Council Decision (EU) 2017/971 of 8 June 2017 setting out the arrangements for planning and conducting EU military missions in the field of CSDP without an executive mandate and amending Decisions 2010/96/CFSP on a European Union military mission to contribute to the training of Somali security forces, 2013/34/CFSP on the European Union military mission to contribute to the training of Malian forces (EUTM Mali) and (CFSP) 2016/610 on the European Union military CSDP training mission in the Central African Republic (EUTM CAR),* 2017.

122 *Council Decision of 22 May 2000 setting up a Committee for the Civilian Aspects of Crisis Management, 2000/354/CFSP,* 2000.

– making recommendations to PSC;
– developing civilian crisis management and civilian capability strategies.

Another EU agency is the Institute for Security Studies, which was established in 2002, and its legal basis is now Council Decision 2014/75/CFSP of 10 February 2014.[123]

The Institute is headquartered in Paris. To facilitate the organisation of its work in Brussels, it also has a liaison office in that city (Article 1(3)).

The Institute's tasks include (Article 2):
– contributing to the development of EU strategic ideas on CFSP and CSDP, particularly conflict prevention and peacebuilding;
– conducting analysis and disseminating knowledge on the CFSP;
– promoting contacts with the academic world, think tanks and relevant civil society actors.

Political oversight of the Institute's activities is exercised by PSC, under the direction of the Council. Operational guidelines for the Institute may be issued by High Representatives (Article 3).

The Institute shall have the legal personality necessary to perform its functions and attain its assigned objectives. In particular, it may enter into contracts, acquire or dispose of movable and immovable property and be a party to legal proceedings. The Institute is not profit-oriented (Article 4).

It works under a Director appointed by its Council (Articles 5–6).

The EU Satellite Centre is another EU agency, established in January 2002 by the Council Joint Action of 20 July 2001.[124]

It is headquartered in Torrejón de Ardoz, Spain (Article 1(2)).

Its tasks include supporting EU decision-making in the field of CFSP, including EU crisis management operations, by providing material derived from the analysis of satellite imagery and ancillary data such as aerial imagery (Article 2).

Political oversight is exercised by PSC, which may make recommendations on the matter (Article 3).

7. CSDP and NATO

Since the Lisbon Treaty, the EU has not only become an organisation of economic and social integration, but also a military alliance. The EU has acquired the capacity to autonomously carry out civilian and military missions for peacekeeping,

123 *Council Decision of 10 February 2014 on the European Union Institute for Security Studies*, 2014.
124 *Council Joint Action of 20 July 2001 on the establishment of the European Union Satellite Centre,* 2001.

conflict prevention and strengthening of international security (Article 42(1) TEU). The Lisbon Treaty also added an obligation to mutual defence (Article 42(7) TEU). According to it, Member States are obliged to assist their counterparts in the event of an "armed attack" on its territory. It also states that 'commitments and cooperation in this area shall be consistent with commitments under NATO, which, for those States that are members of it, remains the foundation of their collective defence and the forum for its implementation'.

This provision refers to Article 5 of the NATO, in which State parties

> agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against all of them, and therefore agree that if such an armed attack occurs, each of them, in the exercise of the right of individual or collective self-defence recognized under Article 51 of the Charter of the United Nations, will render assistance to the Party or Parties attacked by taking promptly, alone as well as in concert with other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Article 4 of the 1948 Brussels Treaty contained a similar clause:

> Should any of the High Contracting Parties become the target of an armed attack in Europe, the other High Contracting Parties shall, in accordance with the provisions of Article 51 of the Charter of the United Nations, render to the party attacked such military and other assistance as is within their power.

The immediate reason for enshrining the self-defence clause in Article 42(7) TEU was the dissolution of WEU and termination of the Brussels Treaty of 1948. In a situation where not all Member States were NATO members in 2009, these States would have been left without security guarantees from other Member States. In addition, the formulation of the self-defence clause in the TEU was the desire of some Member States to strengthen European security space at the expense of non-European NATO Member States.[125]

The transformation of the EU into a political and defence alliance raises the question of its relationship with NATO. Currently, virtually all EU Member States have become NATO members (except for Ireland, Austria and Sweden; however, the latter has the prospect of becoming a NATO member as early as 2024). However, besides one passage in Article 42(7) of TEU, there is no other provision regulating the relationship between the EU and NATO.

The importance of Article 42(7) TEU was underlined by the EU Heads of State and Government at their informal meeting in Versailles in March 2022 in the context of the Russia–Ukraine war.[126] In this declaration, the European Council stressed that

125 Macalister-Smith and Gebhard, 2013.
126 *Informal meeting of Heads of State or Government. Versailles Declaration*, 2022.

a stronger and more capable EU in the field of security and defence would make a positive contribution to global and transatlantic security and would complement NATO, which remains the basis of collective defence for its members. Solidarity between Member States is reflected in Article 42(7) TEU.

The Versailles Declaration of March 2022 is part of the construction of a mutual relationship between the EU and NATO. Over the decades, since the CSDP began to be built, these relations have evolved, with the European Council setting the pace and direction of these ties and their interdependencies.[127]

The first joint meeting of EU and NATO representatives was held on 19 September 2000, between ambassadors of NATO's North Atlantic Council and PSC.[128] The NATO Secretary General underscored the need for complete cooperation between the EU and NATO, while also indicating that building structures and shaping procedures were not substitutes for building adequate defence capabilities. The meeting marked the beginning of regular contacts in this format.

Fundamental decisions on the shape of EU–NATO relations were made at the European Council meeting in Nice.[129] The EU Heads of State and Government decided on the creation of permanent political and military bodies, and their composition, competence and rules of operation. Formal decisions were also adopted through consultation and cooperation between the EU and NATO. The formal expression of cooperation became an exchange of letters in January 2001 between the NATO Secretary-General and the then President of the EU Council.[130] The NATO Secretary-General underlined NATO's willingness to hold at least one NATO–EU ministerial meeting and three North Atlantic Council and PSC meetings during one EU Presidency, as well as expert meetings, military committees and secretariats. He proposed that each organisation could request additional meetings when needed and that the NATO and EU should increase the frequency of their contacts during crises. NATO also announced that representatives of EU Presidency would be invited to meetings organised by NATO. The President of the EU Council confirmed the proposals of the NATO Secretary-General and expressed expectations of further cooperation.

These arrangements were never transformed into a binding international agreement between the two organisations, and the mutual relationship between the EU and NATO was expressed in a series of declarations between 2016 and 2023. These declarations began a new phase in the history of EU–NATO relations and elevated them to the status of a strategic partnership.

The Declaration of 8 July 2016 was signed in Warsaw by the Presidents of the European Council, the President of the European Commission, and the NATO Secretary

127 Bugajski, 2023, p. 95.
128 *Intervention by Dr Javier Solana High Representative for CFSP*, 2000.
129 European Council, 2000.
130 *Exchange of letters between George Robertson, Secretary-General of NATO and Anna Lindh, Swedish FM and Chairman of the Council of the European Union*, 2001.

General.[131] Its aim was to strengthen cooperation in seven areas: combating hybrid threats; operational cooperation in the field of irregular migration; cyber-security and defence; defence capabilities; defence sector and defence research; exercises; and supporting partners' efforts to build capacity in the Western Balkans, Eastern and Southern neighbourhoods, and strengthening their resilience. The Declaration emphasised that cooperation between the EU and NATO would be conducted in the spirit of openness and transparency with full respect for decision-making autonomy and procedures of both organisations and without prejudice to the specific nature of the security and defence policy of any Member State. The 2016 Declaration materialised in the form of the Council Conclusions of 6 December 2016 in which the Member States endorsed a common set of 42 proposals representing concrete actions for the implementation of the Joint Declaration.[132] These were jointly developed by the EU (EEAS, Commission Services and EDA) and NATO.

The second EU–NATO Joint Declaration was signed on 10 July 2018 in Brussels, reaffirming the importance and need for cooperation between the two organisations, and emphasising the mutual benefits of security and defence initiatives. The Declaration highlighted three fields of current cooperation, that is combating smuggling and trafficking of migrants in the Mediterranean, enhancing the capacity to respond to hybrid threats and supporting the defence and security capabilities of our neighbours to the east and south. However, it is imperative to deepen cooperation in new areas such as military mobility; counterterrorism; strengthening resilience to chemical, biological, radiological and nuclear threats; and promoting women's peace and security agendas. The EU's parallel efforts to develop CSDP and NATO's efforts to fulfil the organisation's core tasks received significant support, particularly the need to develop defence capabilities that are coherent, complementary, and interoperable and accessible to both organisations.

The arrangements made therein were reviewed periodically according to both declarations. The final review was conducted in 2022 and covered the period following the Russian invasion of Ukraine.[133] The review report highlighted the progress made in terms of political dialogue and ongoing political consultations in PSC and the North Atlantic Council, and in briefings in various committees and working groups. The report highlighted the results of joint work in agreed-upon areas (including strategic communications and countering information manipulation, and interference by foreign actors). The Seventh Report also noted the adoption of the EU Strategic Compass.

The next EU–NATO Joint Declaration of Cooperation was signed on 10 January 2023, where they noted that their strategic partnership is based on shared values,

131 *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 2016.

132 European Council, 2016.

133 *Seventh progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017*, 2022.

determination to face common challenges, and an unequivocal will to promote and protect peace, freedom and prosperity in the Euro–Atlantic region. Both organisations noted the security threat posed by Russia's aggression against Ukraine and the People's Republic of China's policies. In the current situation, transatlantic ties are becoming increasingly important than ever before, necessitating closer EU–NATO cooperation. The Declaration emphasised NATO's overarching role in Euro–Atlantic security, recalling that NATO remains the foundation of allies' collective defence, while EU capabilities are complementary and interoperable with NATO. As security threats and challenges facing the EU and NATO evolve in scope and scale, the two organisations have pledged to take their partnership to the next level, strengthen cooperation in existing fields and expand it, notably on increasing geostrategic competition, resilience challenges, critical infrastructure protection, new and disruptive technologies, space, the security implications of climate change and foreign information manipulation and interference.

References

I. Literature

Anand, R.P. (1986) 'Sovereign Equality of States in International law' in *Collected Courses of the Hague Academy of International Law*. Volume 197.

Bloed, A., Wessel, R.A. (1994) *The Changing Functions of the Western European Union (WEU): Introduction and Basic Documents***.** Dordrecht/Boston/London: Martinus Nijhoff Publishers; https://doi.org/10.1163/9789004641075_004.

Bugajski, A. (2023) *Problemy i wyzwania w stosunkach NATO – Unia Europejska* [Problems and Challenges in NATO-European Union Relations]. Warsaw: *Polski Instytut Stosunków Międzynarodowych*.

Butler, G. (2021) *Constitutional Law of the EU's Common Foreign and Security Policy. Competence and Institutions in External Relations*. London: Bloomsbury Publishing.

Cassese, A. (2001) *International Law*. Oxford: Oxford University Press.

Contartese, C. (2017) 'The Autonomy of the EU Legal Order in the ECJ's External Relations Case Law: From the "Essential" to the "Specific Characteristics" of the Union and Back Again', *Common Market Law Review*, 54(6), pp. 1627–1671; https://doi.org/10.54648/COLA2017145.

Cremona, M. (2018) 'The position of CFSP/CSDP in the EU's constitutional architecture' in Blockmans, S., Koutrakos, P. (eds.) *Research Handbook on the EU's Common Foreign and Secutrity Policy*. Cheltenham: Elgar, pp. 5–21; https://doi.org/10.4337/9781785364082.00008.

Eckes, Ch. (2015) 'The CFSP and Other EU Policies: A Difference in Nature?', *European Foreign Affairs Review*, 20(4), pp. 535–552; https://doi.org/10.54648/eerr2015044.

Eckes, Ch. (2016) 'Common Foreign and Security Policy: The Consequences of the Court's Extended Jurisdiction', *European Law Journal*, 22(4), pp. 492–518; https://doi.org/10.1111/eulj.12183.

Gadkowski, A., Gadkowski, T. (2019) 'Wspólna Polityka Zagraniczna i Bezpieczeństwa Unii Europejskiej po reformach traktatowych' [The European Union's Common Foreign and Security Policy after the Treaty Reforms] in Cała-Wacinkiewicz, E., Menkes, J., Nowakowska-Małusecka, J., Staszewski, W.S. (eds.) *W jakiej Unii Europejskiej Polska – jaka Polska w Unii Europejskiej. Instytucjonalizacja współpracy międzynarodowej* [In what kind of European Union Poland – what kind of Poland in the European Union. Institutionalization of international cooperation]. Warszawa: C.H. Beck, pp. 87–106.

Geiger, R., Khan, D.-E., Kotzur, M. (eds.) (2015) *European Union Treaties*. 1st edn. Oxford: Hart Publishing.

Geradin, D. (2015) 'The external relations of the European Union and its Member States. Lessons from recent developments in the economic sphere' in Chinkin, Ch., Baetens, F. (eds.) *Sovereignty, Statehood and State Responsibility. Essays in Honour of James Crawford*. Cambridge: Cambridge University Press, pp. 406–420; https://doi.org/10.1017/CBO9781107360075.028.

Hillion, Ch., Wessel, R. (2009) 'Competence distribution in EU external relations after Ecowas: Clarification or continued fuzzines?', *Common Market Law Review*, 46(2), pp. 551–586; https://doi.org/10.54648/COLA2009023.

Hillion, Ch., Wessel, R. (2018) ''The Good, the Bad and the Ugly': three levels of judicial control over the CFSP' in Blockmans, S., Koutrakos, P. (eds.) *Research Handbook on the EU's Common Foreign and Security Policy.* Cheltenham: Edward Elgar; https://doi-org.peacepalace.idm.oclc.org/10.4337/9781785364082.

Howorth, J.M. (2012) 'European Security Institutions 1945-2010: The Weaknesses and Strengths of 'Brusselsisation'' in Biscop, S., Whitman, R. (eds.) *The Routledge Handbook of European Security.* London: Routlegde; pp. 5–17.

Kellerbauer, M., Klamert, M., Tomkin, J. (2019) *The EU Treaties and the Charter of Fundamental Rights: A Commentary.* Oxford: Oxford Academic; https://doi.org/10.1093/oso/9780198794561.001.0001.

Koutrakos, P. (2013) *The EU Common Security and Defence Policy.* Oxford: Oxford University Press; https://doi.org/10.1093/acprof:oso/9780199692729.001.0001.

Kwiecień, R. (2004) *Suwerenność państwa. Rekonstrukcja i znaczenie idei w prawie międzynarodowym* [State Sovereignty: Reconstruction and Significance of the Idea in International Law]. Zakamycze: Wolters Kluwer.

Lonardo, L. (2023) *EU Common Foreign and Security Policy After Lisbon: Between Law and Geopolitics.*, Cham: Springer; https://doi.org/10.1007/978-3-031-19131-2.

Macalister-Smith, P., Gebhard, J. (2013) 'Western European Union (WEU)' in Rüdiger, W. (ed.) *Max Planck Encyclopedias of International Law [MPIL].* 2nd edn. Oxford: Oxford University Press online.

Marquardt, S. (2018) 'The institutional framework, legal instruments, and decision-making procedures' in Blockmans, S., Koutrakos, P. (eds.) *Research Handbook on the EU's Common Foreign and Secutrity Policy*, Cheltenham: Elgar, pp. 22–43; https://doi.org/10.4337/9781785364082.00009.

Mik, C. (2000) *Europejskie prawo wspólnotowe. Zagadnienia teorii i praktyki. Tom 1.* [European Community Law. Issues of theory and practice. Volume 1.]. Warszawa: C.H. Beck.

Mik, C. (2022) *Państwo i prawo wobec procesów internacjonalizacji, integracji i globalizacji. Tom 1. Wpływ internacjonalizacji i integracji na klasyczny paradygmat państwa i prawa* [State and Law in the Face of the Processes of Internationalization, Integration and Globalization. Volume 1 The impact of internationalization and integration on the classical paradigm of state and law]. Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora.

Mikos-Sitek, A. (2022) 'Common Foreign, Security and Defense Policies' in Osztovits, A., Bóka, J. (eds.) *The Policies of the European Union from a Central European Perspective.* Miskolc-Budapest: CEA Publishing, pp. 197–215; https://doi.org/10.54171/2022.aojb.poeucep_10.

Muszyński, M. (2011) *Państwo w prawie międzynarodowym. Istota, rodzaje i atrybuty* [State in international law. Essence, types and attributes]. Bielsko-Biała: Wydawnictwo STO.

Neuhold, H. (2013) 'European Common Foreign and Security Policy' in Rüdiger, W. (ed.) *Max Planck Encyclopedias of International Law [MPIL].* 2nd edn. Oxford: Oxford University Press.

Schmidt, J. (2020) *The European Union and the Use of Force*. Leiden: Koninklijke Brill NV; https://doi.org/10.1163/9789004356078.

de Waele, H. (2023) *Legal Dynamics of EU External Relations. Dissecting a Layered Global Player. Third Edition.* Berlin/Heidelberg: Springer; https://doi.org/10.1007/978-3-662-67593-9.

Wouters, J., Hoffmeister, F., De Baere, G., Ramopoulos, T. (2021) 'Common Foreign and Security Policy.' in Wouters, J., Hoffmeister, F., De Baere, G., Ramopoulos, T. (eds.) *The Law of EU External Relations: Cases, Materials, and Commentary on the EU as an International Legal Actor.* Oxford: Oxford University Press; https://doi.org/10.1093/oso/9780198869481.001.0001.

II. Judgments and decisions

Judgment of the Constitutional Court of 24 November 2010, OTK ZU 9A/2010, item 108.
Judgment of the Court of Justice (Grand Chamber) of 14 June 2016, C-263/14, *European Parliament v Council*, ECLI:EU:C:2016:435.
Judgment of the Court of Justice (Grand Chamber) of 26 November 2014, C 103/12 and C 165/12, *European Parliament, and European Commission v Council*, ECLI:EU:C:2014:2400.
Judgment of the Court of Justice of 10 December 2018, C-621/18, *Andy Wightman and Others v Secretary of State for Exiting the European Union*, ECLI:EU:C:2018:999.
Judgment of the Court of Justice of 12 September 2017, *Alexios Anagnostakis v European Commission*, C-589/15 P (ECLI:EU:C:2017:663).
Judgment of the Court of Justice of 15 December 2009, C-461/05, *European Commission v. Denmark*.
Judgment of the Court of Justice of 19 July 2012, C-130/10, *European Parliament v Council*, EU:C:2012:472.
Judgment of the Court of Justice of 24 June 2014, C-658/11, *European Parliament v Council*, EU:C:2014:2025.
Judgment of the Court of Justice of 25 June 2020, C-14/19 P, *European Union Satellite Centre,* ECLI:EU:C:2020:492, § 60.
Judgment of the Court of Justice of 28 March 2017, C-72/15, *Rosneft,* ECLI:EU:C:2017:236.
Judgment of the Court of Justice of 4 December 1974, 41/74, *Yvonne van Duyn p. Home Office*, ECLI:EU:C:1974:133.
Judgment of the Court of Justice of 4 September 2018, C-244/17, *European Commission v Council*, EU:C:2018:662.
Judgment of the Court of Justice of 6 October 2020, C-134/19 P, *Bank Refah Kargaran,* ECLI:EU:C:2020:793.
Judgment of the General Court (Grand Chamber) of 27 July 2022, T 125/22, *RT France v Council of the European Union*, ECLI:EU:T:2022:483.
Judgment of the General Court of 4 June 2014, T 67/12, *Sina Bank v Council*, EU:T:2014:348.
Opinion of the Court of Justice 1/09 of 8 March 2011, ECLI:EU:C:2011:123.
Opinion of the Court of Justice 2/13 of 18 December 2014, ECLI:EU:C:2014:2454.
Opinion of the Court of Justice of 30 November 2009, 1/08, ECLI:EU:C:2011:123, §§ 108–109.
Opinion of the Court of Justice of 4 October 1979, 1/78, European Court reports 1979 Page 02871
Permanent Court of International Justice, *S.S. "Wimbledon" Case*, Serie A, no. 1.

III. Treaties and other international documents

22 Meeting of European Union Defence Ministers (2000) Sintra, 28 February 2000.
Council Decision (CFSP) 2015/1835 of 12 October 2015 defining the Statute, seat and functioning of the European Defence Agency (recast) (2015) OJ L 266, 13 October 2015.

Council Decision (EU) 2017/971 of 8 June 2017 setting out the arrangements for planning and conducting EU military missions in the field of CSDP without an executive mandate and amending Decisions 2010/96/CFSP on a European Union military mission to contribute to the training of Somali security forces, 2013/34/CFSP on the European Union military mission to contribute to the training of Malian forces (EUTM Mali) and (CFSP) 2016/610 on the European Union military CSDP training mission in the Central African Republic (EUTM CAR) (2017) OJ L 146, 9 June 2017.

Council Decision of 10 February 2014 on the European Union Institute for Security Studies (2014) 2014/75/CFSP, OJ L 41, 12 February 2014.

Council Decision of 22 January 2001 on the establishment of the Military Staff of the European Union (2001) 2001/80/CFSP, OJ L 27, 30 January 2001.

Council Decision of 22 January 2001 setting up the Military Committee of the European Union (2001) 2001/79/CFSP, OJ L 27, 30 January 2001.

Council Decision of 22 May 2000 setting up a Committee for the Civilian Aspects of Crisis Management (2000) 2000/354/CFSP, OJ L 127, 27 May 2000.

Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010) 2010/427/EU, OJ L 201, 3 August 2010.

Council Joint Action of 20 July 2001 on the establishment of a European Union Satellite Centre (2001) 2001/555/CFSP, OJ L 200, 25 July 2001.

Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (1970) A/RES/2625(XXV), 24 October 1970.

European Council (1989) 'Conclusions of the Presidency' Strasbourg, 8 and 9 December 1989.

European Council (1997) 'Conclusions of the Presidency' Amsterdam, 16 and 17 June 1997.

European Council (1999a) 'Conclusions of the Presidency' Cologne, 3 and 4 June 1999, Annex III.

European Council (1999b) 'Conclusions of the Presidency' Helsinki, 10 and 11 December 1999.

European Council (2000a) 'Conclusions of the Presidency' Santa Maria da Feira, 19 and 20 June 2000.

European Council (2000b) 'Conclusions of the Presidency' Nice, 7-9 December 2000.

European Council (2001) 'Conclusions of the Presidency' Laeken, 14 and 15 December.

European Council (2003) 'Conclusions of the Presidency' Thessaloniki, 19 and 20 June 2003.

European Council (2016) 'Council Conclusions on the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary-General of the North Atlantic Treaty Organisation' Brussels, 6 December 2016.

European Council (2017) 'Council conclusions on progress in implementing the EU global security and defence strategy' *Press Release*, Brussels, 6 March 2017.

Exchange of letters between George Robertson, Secretary-General of NATO and Anna Lindh, Swedish FM and Chairman of the Council of the European Union (2001) 24 January 2001.

Informal meeting of Heads of State or Government. Versailles Declaration (2022) Versailles, 10 and 11 March 2022.

Intervention by Dr Javier Solana High Representative for CFSP (2000) COPSi/NAC first joint meeting, Brussels, 19 September 2000.

Joint Declaration on European Defence, Joint Declaration issued at the British-French Summit (1998) Saint-Malo, 4 December 1998. [Online]. Available at: https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf (Accessed: 5 January 2024).

Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization (2016) *Press Release*, (2016) 119, 8 July 2016.

Protocol Modifying and Completing the Brussels Treaty (Western European Union) (1954) Paris, 23 October 1954.

Seventh progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017 (2022) 20 June 2022. [Online]. Available at: https://www.consilium.europa.eu/media/57184/eu-nato-progress-report.pdf (Accessed: 5 January 2024).

Single European Act (1987) OJ L 169, 29 June 1987.

Statement of the Presidency of the Permanent Council of the WEU on behalf of the High Contracting Parties to the Modified Brussels Treaty – Belgium, France, Germany, Greece, Italy, Luxembourg, The Netherlands, Portugal, Spain and the United Kingdom (2010) Brussels, 31 March 2010.

The Treaty of Economic, Social and Cultural Collaboration and Collective Self-Defence (1948) Brussels, 17 March 1948. [Online]. Available at: https://www.cvce.eu/en/obj/the_brussels_treaty_17_march_1948-en-3467de5e-9802-4b65-8076-778bc7d164d3.html (5 January 2024).

Treaty of Amsterdam (1997) OJ C 340, Amsterdam, 10 November 1997.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (2007) OJ C 306, Lisbon, 17 December 2007.

Treaty of Nice (2001) OJ C 80, Nice, 10 March 2001.

Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations (1986) 21 March 1986.

Western European Union Council of Ministers (1992) 'Petersberg Declaration' Bonn, 19 June 1992, Brussels: *Press and Information Service*.

Part III

LEGAL ASPECTS OF INVESTMENT AND FINANCING

Chapter 5

Legal Aspects of Defence Procurement in the European Union: Funding Incentives and Regulatory Shields

Bálint Kovács

'Every gun that is made, every warship launched, every rocket fired signifies,
in the final sense, a theft from those who hunger and are not fed,
those who are cold and are not clothed.
This world in arms is not spending money alone.
It is spending the sweat of its laborers, the
genius of its scientists, the hopes of its children.'
Dwight D. Eisenhower

Abstract

This chapter presents an analysis of regulations established at the European Union level, particularly aimed at improving common defence capabilities by encouraging industrial development. It critically examines the specific instruments utilised by States in the course of defence procurement. First, it focuses on the "Defence Package", outlining the purpose and content of this regulatory attempt to harmonise Member States' legislation on the procurement and transfer of defence-related products. It then analyses the potential reasons for its limited application. This is followed by an inquiry into the potential for funding schemes to act as incentives to boost cooperative defence spending and encourage Member States to engage in the harmonised development of the European defence industry. The analysis also briefly evaluates the situation of small and medium-sized enterprises, particularly those within the novel funding schemes. Finally,

Bálint Kovács (2024) 'Legal Aspects of Defence Procurement in the European Union: Funding Incentives and Regulatory Shields'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 215–253. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_5

it addresses the specific instruments regularly used by States in defence procurement, with an emphasis on defence offsets as a means for defence industrial protectionism.

Keywords: defence package, procurement, transfers, funding, SMEs, offsets

1. Introductory remarks: policy abundance, implementation dearth

The defence capabilities of the European Union (EU) and its Member States have often been analysed through the prism of their partnership with or membership in the North Atlantic Treaty Organization (NATO). This approach has so often been criticised in the media, that citation is not even warranted: the EU is overly reliant on the United States as a guarantor of its security. Criticism regarding modest defence spending by European members of NATO has also been highlighted by the media in recent years. However, since the war returned to Europe, even the most dovish of EU Member States have augmented their defence spending, or have at least committed to doing so. The question now is, how best to spend this money? How best do you fulfil these commitments? The challenges are numerous, as industrial capacity has waned, not least because of the incongruence in spending priorities.[1] The ramp-up in spending comes at a time when the EU's pursuit of *strategic autonomy* also reappeared on the agenda with greater vigour. The concept of strategic autonomy re-entered public consciousness at a time when EU leaders were wary of NATO's direction.[2] This concept is now part of the EU's security and defence aims. The recent ramp-up in defence spending[3] may well be attributed to crises at European borders, but increased spending must nevertheless be accompanied by increased cooperation.

Coordinating defence and security efforts has been on the EU agenda since its inception. The idea evolved over the decades,[4] with common defence being developed as part of the Common Foreign and Security Policy (CFSP), and included in the Maastricht Treaty. This was then carried over through the Treaty of Lisbon into Chapter 2, Section 2 of the Treaty on European Union (TEU). A principal component of CFSP is Common Security and Defence Policy (CSDP), also known as the European Defence Union (EDU). The CSDP represents a platform through which EU Member States can combine resources to implement joint initiatives. Since its inception, numerous initiatives have been undertaken to give content to this cooperation. This includes the

1 As also acknowledged in European Commission, 2022, p. 1.

2 French President Emmanuel Macron expressed concerns that '[w]hat we are currently experiencing is the brain death of NATO'. As quoted in The Economist, 2019.

3 NATO, 2023.

4 Through initiatives such as the Western European Union's Petersberg tasks (Petersberg Declaration) or the Berlin Plus agreement.

European Security Strategy (ESS), which was first developed in 2003. However, despite its holistic approach to the questions of security and defence, it has overlooked an extremely important aspect of this cooperation: coordination in terms of defence procurement. The ESS was replaced by the EU Global Strategy in 2016, through which the importance of "concerted and cooperative effort" in defence spending became a major theme in CSDP.

Coordinated defence spending promises to enhance output and industrial growth. Therefore, it becomes a necessary tool for achieving strategic autonomy.[5] Further policies and platforms have appeared to buttress such cooperation. The Treaty of Lisbon established the European External Action Service, a common structure created to carry out CSDP, among others. The Treaty also includes a mutual defence clause and introduces Permanent Structured Cooperation (PESCO) for Member States wishing to pursue defence integration. PESCO was first initiated in 2017 with the aim of increasing defence cooperation at a new level. Enhanced cooperation through PESCO, together with the Coordinated Annual Review on Defence (CARD), European Defence Fund (EDF), and Military Planning and Conduct Capability, are the main components of EU defence cooperation. Their activity is underpinned and coordinated by the European Defence Agency (EDA), which has been in existence since 2004, as well as the Directorate-General for Defence Industry and Space.

The aforementioned details are meant only as a brief stocktaking and are not aimed at providing a complete inventory;[6] however, they illustrate that defence-related policies at the EU-level seem to be as fragmented as the EU defence market. This convoluted web of platforms and policies was intended to enable deeper cooperation among Member States under the brokerage of the EU. Furthermore, it is possible that without this convoluted web of platforms for coordinating political will, implementation of *jus cogens* defence-related instruments such as the "Defence Package", would face severe shortfalls. These endeavours point to a European Commission that is expanding its role in the area of defence, both to bolster the capabilities of Member States, to secure the EU itself and to boost the European defence industry to generate growth.[7]

The number of documents addressing collective security matters has also increased. However, to what end? Recognising the importance of the industry in achieving common defence goals, the EDA advanced the Strategy for the European Defence Technological and Industrial Base (EDTIB) in 2007. Member States adopted the EDTIB Strategy, which aimed to integrate national defence technological and industrial bases to achieve self-sufficiency for security of supply at the EU level.[8] Six years after the EDTIB Strategy was agreed upon, a study by the European Commission's Directorate-General for External Policies of the Union analysed its progress.

5 European External Action Service, 2016, pp. 20, 45.
6 For a review of key defence policy instruments, see: Csiki Varga, 2024, starting at p. 207.
7 Britz, 2023, p. 217.
8 Directorate-General for External Policies of the Union, 2013, p. 8.

The analysis examined the trends dominating the European defence industry, and provided a grim outlook regarding the implementation of the strategy. The study called for a revision of EDTIB, as well as new policies to protect "key industrial capacities", changes to funding and investment methods, and the use of structural and cohesion funds in relation to EDTIB. It highlighted the importance of harmonising demand, synchronising procurement and engaging in joint research and technology projects to develop EDTIB.[9] When the study was released, European economic policy was dominated by austerity, aimed at countering and addressing the prolonged effects of the Great Recession and European debt crisis. The dire economic situation only accelerated the trend of decreasing national defence spending of Member States.[10] The European Commission's analysis openly stated that implementing the EDTIB Strategy was "increasingly unlikely".[11] Over ten years have passed since the analysis was published, and effective cooperation between Member States seems to be stranded among the myriad plans and political declarations of intent.

It took an acute crisis to reignite discussions and willingness to engage in planning for common defence priorities at the EU level. Europeans are now more concerned about their safety than they have been for a long time, which leaves little opposition to increased defence spending and deepening of EU-wide defence cooperation. A recent poll by Eurobarometer, the official polling instrument of the European Parliament, shows that over three-quarters of Europeans favour common defence and security policies. Deepening cooperation within the EU on defence matters received overwhelming support (80%), while two-thirds said more funds should be earmarked for defence.[12] It seems that it is the appropriate time to make progress and deepen EU-wide cooperation in defence. This is particularly true in terms of increasing defence budgets and improving spending coordination. As this chapter demonstrates, leaders of EU Member States have only profited from the present opportunity to a limited extent. Political statements continue to outshine action, although there is a sense of urgency that has ignited recent actions.

The defence spending of individual EU Member States has increased significantly in the past couple of years compared to the period before Russia's invasion of Ukraine in 2022.[13] This is significant, as governments' buying power is an important determinant of the ownership, size, structure and performance of national defence industries. While it is important that Member States improve their military capabilities, coordinated spending would be more beneficial to this end. Although Member States have repeatedly acknowledged this, increased spending at the EU level has seemingly pitted them against each other in a sort of *friendly arms race*. This once again brought to the fore previously-identified challenges. These are general challenges related to

9 Ibid., p. 11.
10 Ibid., pp. 13–14.
11 Ibid., p. 10.
12 *Standard Eurobarometer 99 – Spring 2023*, 2023.
13 NATO, 2023.

the EU budget, such as calculating cost-benefit aspects or overcoming the *juste retour* dilemma, as well as substantial legal limitations. In addition, specific issues relate to the defence industry itself, or rather with its protection at the national level, as well as the lack of coordination between national authorities. Deficiencies in cooperation appear as manifestations of a deeper issue, considering that steps have been taken to harmonise procurement rules along the lines of market logic.

This chapter focuses on analysing regulations established at the EU level, specifically aimed at improving common defence capabilities by encouraging industrial development. It critically examines the specific instruments utilised by States during the course of defence procurement. First, it focuses on the "Defence Package", elucidating the purpose and content of this regulatory attempt at harmonising Member States' legislation on procurement and transfer of defence-related products. It then analyses the potential reasons for its limited application. This is followed by an inquiry into the potential for funding schemes to act as incentives for boosting cooperative defence spending and encouraging Member States to engage in the harmonised development of the European defence industry. This analysis separately, albeit briefly, evaluates the situation of small and medium-sized enterprises (SMEs), and focuses on these companies within the novel funding schemes. The chapter also provides an overview of specific instruments used regularly by States in the course of their defence procurement endeavours, focusing in particular on defence offsets. The chapter ends with concluding remarks by the author.

2. The "Defence Package": the glass half empty

Identifying the precise line in the division of competences within the EU may sometimes prove to be challenging. Although the division of competences seems obvious at first glance, when one examines the details of a particular area that appears to constitute the sole competence of Member States, one may nevertheless run into regulation from the EU. This is how the field of defence and security appears. Without delving into all the political iterations of EU institutions, especially the European Commission, in terms of improving the functioning of the internal market, two directives must be highlighted. Directive 2009/81/EC[14] provides procurement rules specifically aimed at defence and security markets, while Directive 2009/43/EC[15] contains rules on the intra-EU transfer of defence-related products.

14 *Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC*, 2009.

15 *Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community*, 2009.

The Defence Package, as the two Directives were collectively called, is described in the subsections below, highlighting its most important features. The aim of the Defence Package was to create a European Defence Equipment Market (EDEM) along the lines of market logic in congruence with fundamental freedoms. Although it appears suitable for this purpose, the results achieved thus far demonstrate that there is nevertheless room for improvement.

2.1. Procurement rules

It is not an understatement that procurement in the defence and security sectors has traditionally been opaque. The Treaty on the Functioning of the European Union (TFEU) includes an exception clause in Article 346[16] that Member States may use to maintain the confidentiality of defence procurement, among others. As demonstrated herein, this exception clause is front-and-centre when it comes to old, ingrained habits of secrecy and protectionism in defence procurement being perpetuated. These habits are nevertheless present, despite efforts at the EU level aimed at improving European companies' access to Member States' defence markets by promoting fair and transparent practices in the procurement of defence-related products. EU Member States continue to use Article 346 apparently without restrictions to exercise economic protection and avoid the application of EU procurement rules in the defence sector.

The European Commission devised a plan to establish EDEM, aiming to strengthen EDTIB and develop its military capabilities. Accordingly, the European Commission considered it essential that the rules for procurement in the defence and security markets be harmonised. It advanced a proposal for a directive that was to become Directive 2009/81/EC (hereinafter the "Defence Procurement Directive" or "DPD"), aiming to enhance competition and transparency in this field, while limiting the use of Article 346 TFEU (or Article 296 at the time the Directive was drafted).[17]

DPD seeks to open up Member States' defence markets in front of defence companies based in other Member States. The scope of DPD was established in Article 2, and it is clear that the Commission was not reticent, ensuring that it includes as wide a range of contracts as possible in the areas of defence and security. Therefore,

16 Article 346 TFEU reads as follows:
1. The provisions of the Treaties shall not preclude the application of the following rules:
(a) no Member State shall be obliged to supply information, the disclosure of which it considers contrary to the essential interests of its security;
(b) any Member State may take such measures as it considers necessary for the protection of the essential interests of its security, which are connected with the production of or trade in arms, munitions and war material; such measures shall not adversely affect the conditions of competition in the internal market regarding products which are not intended for specifically military purposes.
2. The Council may, acting unanimously on a proposal from the Commission, make changes to the list, which it drew up on 15 April 1958, of the products to which the provisions of paragraph 1(b) apply.

17 Recital 2, 4 and 20 of the Defence Procurement Directive.

DPD applies to contracts in the following areas: (a) the supply of military equipment, including any parts, components and/or subassemblies thereof; (b) the supply of sensitive equipment, including any parts, components and/or subassemblies thereof; (c) works, supplies and services directly related to the equipment referred to in points (a) and (b) for any and all elements of its life cycle; and (d) works and services specifically for military purposes or sensitive works and services.[18] In terms of the value of the contracts, Article 8 establishes the thresholds for the application of DPD as follows: (a) 421,000 euros for supply and service contracts and (b) 5,150,000 euros for works contracts (excluding VAT in both cases). Considering the numbers involved in defence procurements, these thresholds appear to bring the vast majority of Member States' defence procurements under the purview of DPD. Chapter II, Section 3 of the DPD contains provisions on excluded contracts. Such exemptions include certain government-to-government contracts, as per Article 13(f) of the DPD; or co-operative research and development programmes, as per Article 13(c) of the DPD; or contracts awarded pursuant to rules contained in other international agreements (such as NATO). Another category of exemptions includes contracts governed by the rules of an international agreement between Member States and third countries, and contracts governed by the rules of an international organisation purchasing for its purpose, as per Articles 12(a) and (c) of the DPD. Such agreements and organisations may include the Organisation for Joint Armament Co-operation, the Letter of Intent Framework Agreement (LoI), or NATO's Support and Procurement Agency (NSPA).[19] These rules appear to allow Member States room for manoeuvre, considering the complexity and sensitive nature of defence procurements. An exemption that is worth noting is made in the case of a 'contract for which the application of the rules of this Directive would oblige a Member State to supply information, the disclosure of which it considers contrary to the essential interests of its security.'[20] Similar to Article 346 TFEU exception, this exemption also allows for the invocation of essential security interests, which may also be prone to abuse. However, the issues surrounding the application of DPD are far greater than this exemption.

Chapter V of DPD contains rules pertaining to the procedures for awarding contracts. Contracting authorities must publish contract notices in the Tenders Electronic Daily (TED) database. Except for somewhat narrowly-defined exclusions, contracting authorities must award procurement contracts in accordance with one of the procedures laid down in Article 25 of the DPD. Contract awards within the scope of the application of DPD must adhere to the principles of equal treatment and transparency to ensure fair competition. It also lays down extensive rules for cases

18 Recital 10 and 11 of the Defence Procurement Directive contain further indications as to the interpretation of its scope.

19 A more extensive view on these exemptions is contained in: Friton, Wolters and Andree, 2020, pp. 28–39.

20 Article 13(a) of the Defence Procurement Directive.

in which contracting authorities may wish to include in their tender 'particulars' in order to safeguard security of information and security of supply.[21]

DPD was published in the Official Journal of the European Union (OJEU) on 21 August 2009 with a deadline of two years for its transposition by Member States. As shown by a Commission report published in October 2012, all but three Member States missed this deadline, prompting the Commission to bring infringement proceedings against them.[22] Complete transposition of DPD was only accomplished by May 2013.[23] A research paper analysed contract notices and awards that appeared in the TED, starting from the entry into force of DPD in August 2011 and the end of 2014. According to this paper, in the first few years of the Directive's implementation it was mostly used for 'contracts dealing with services, acquisition of equipment deemed to be of a low strategic value and sub-systems'.[24] At that time, only a handful of Member States were responsible for the vast majority of TED publications pursuant to DPD. The empirical research presented in the paper shows that major contracts that had a structural effect on EDTIB were made outside the Directive. This means that the DPD did not manage to curb the use of Article 346 TFEU exception, and had limited overall effect on the *culture of secrecy* that characterises military procurement.[25] This can be attributed due in part to the incomplete transposition of DPD, as well as its novelty. In this regard, however, the cited paper's authors expressed their concerns that even those Member States that did implement the Directive may feel discouraged and may thus be driven to change their attitudes and turn in the direction taken by the larger majority that did not apply it.[26] While the paper recognised that it was too early at the time of their analysis for significant conclusions to be drawn, it held that the DPD marked an important step in the procurement policy related to a sector as opaque as defence.[27] Almost a decade later, it is clear that despite their hopes, the same conclusions may still be drawn.

The European Commission conducted its own evaluation of the implementation of DPD, tapping into a wider range of sources such as consultations with the public, stakeholders and Member States.[28] In its report, the European Commission struck an optimistic note, stating that contracts awarded on the basis of the Directive amounted to over 30 billion euros in 2011–2015. However, the report also acknowledges that the total defence procurement expenditure of EU Member States and European Economic Area countries in the same period was approximately 81 billion euros per

21 Articles 22 and 23 of the Defence Procurement Directive.
22 European Commission, 2012.
23 European Commission, 2016b, p. 3.
24 Masson and Martin, 2015, pp. 5, 38.
25 Ibid., p. 38.
26 Ibid., p. 38. In a similar note, see: *Motion for a European Parliament Resolution on the implementation of Directive 2009/81/EC*, concerning procurement in the fields of defence and security, and of Directive 2009/43/EC, concerning the transfer of defence-related products, 2019/2204(INI), para. 11.
27 Masson and Martin, 2015, p. 36.
28 European Commission, 2016b, p. 2.

year.[29] According to the European Commission, the main explanation for this was the unevenness of the DPD's application across Member States, as demonstrated by the fact that only a handful of them were responsible for the vast majority of award notices.[30]

The European Commission's report also analysed numbers regarding cross-border procurement, which demonstrated that 'around 10% of the value of contracts awarded under the Defence Procurement Directive has been won directly by foreign companies'.[31] The efforts undertaken to stimulate competition via the DPD and, in this manner, to bring more opportunities to SMEs was not effective in this initial phase, the European Commission concluded.[32] In terms of DPD's efficiency, consultations conducted by the European Commission revealed that stakeholders considered the costs to outweigh benefits. Nevertheless, the European Commission concluded that the DPD is "broadly efficient" in terms of cost and savings estimations.[33] This conclusion is a *glass half full* reading of the Directive's efficiency when constructive criticism would surely be in order.

Nonetheless, the limited success demonstrated by the implementation of DPD was recognised by the European Commission at the time of drafting the report. The report attributed it to the novelty of the rules and their uneven and partial use, as previously stated.[34] This being the case, the European Commission concluded that, 'overall the text of the Directive is fit for purpose, that the Directive is broadly on track towards meeting its objectives and that an amendment of the Directive is not necessary.'[35] In this sense, the issue is not the regulatory effort in itself; the DPD is fit for purpose, both textually and legally. The main impediment continues to be identified as being the conduct of Member States' authorities. Despite willingness from Member States to operate defence procurements in the EU internal market dimension, it is clear that they were actually unwilling to abandon protectionist practices.

Both the cited paper and the European Commission's report, which were drawn upon, underline that one of the main impediments to fully applying DPD is the continued use of Article 346 TFEU[36] and the broad interpretation of other exemptions mentioned herein.[37] A list, that is referred to in Article 346(2), contains the items to which the exception clause applies.[38] Scholars have noted that this list constitutes the source of further complications, not least because it was actually never published

29 Ibid., pp. 2–3.
30 Ibid., pp. 3–4.
31 Ibid., p. 5.
32 Ibid., pp. 7–8.
33 Ibid., pp. 8–9.
34 Ibid., pp. 5–6, 10.
35 Ibid., p. 10.
36 Masson and Martin, 2015, p. 38.
37 European Commission, 2016b, p. 6.
38 See: Extract of the Council Decision 255/58 of 15 April 1958.

in the OJEU, and its various versions circulating in the public domain also contain some differences.[39] The Court of Justice of the European Union (CJEU) has extensive jurisprudence regarding the use of Article 346 TFEU exception. The CJEU has repeatedly reiterated that security exclusions are exhaustive and must be interpreted narrowly.[40] Jurisprudence also underlines that this exception does not apply to dual-use products.[41] However, this does not preclude their use, nor does it change exclusionary practices.

It is also worth noting that the European Commission published an interpretative communication on the application of Article 346 (then Article 296) exception back in 2006.[42] This was prior to DPD, or the Treaty of Lisbon. Therefore, it may be concluded that Member States chose to maintain these "loopholes", and consequently the possibility of exercising protectionism in defence procurement. There is also an inherent disadvantage in attempting to police the practice of utilising exclusions from DPD. The mentioned interpretative communication underlines that Member States are obliged to 'provide, at the Commission's request, the necessary information and prove that exemption is necessary for the protection of their essential security interests.'[43] This simple observation bears various consequences: Member States may continue using the exemption under Article 346, bearing the risks of what a potential *ex post* investigation may determine. These *ex post* investigations may have even more *potential*, depending on the disposition of the European Commission to initiate them. It is likely that, in a crisis situation such as the current one, the European Commission may feel inclined to turn a blind eye to the extensive use of the exception.

The challenges previously mentioned have endured over time, as demonstrated by a third evaluation and report on the implementation of the DPD elaborated upon the request of the European Parliament, which entrusted a rapporteur with this task in November 2019.[44] The report states that:

> several Member States introduced in their legislation a specific procedure applying to contracts covered by article 346(1)(b) TFEU, still making it difficult to assess whether the article 346 exception has been used for justified reasons of protection of national essential security interests, or just as a way to limit the application of Directive 2009/81/EC.[45]

The report noted that cross-border penetration and SME participation in defence contracts is insufficient, as is the level of cooperation within the EU regarding

39 Trybus, 2014, pp. 91–92.
40 These are analysed *in extenso* in Trybus, 2014, pp. 94–127.
41 Trybus, 2014, pp. 94–95, citing Case T-26/01, *Fiocchi Munizioni SpA v. Commission of the European Communities*, at para. 61.
42 See: European Commission, 2006.
43 Ibid., p. 8.
44 Schwab, 2021, p. 4/25.
45 Ibid.

defence capabilities. Despite the continued challenges, the report also shares positive developments in terms of an increase in the number of contract notices and contract award notices in TED, as well as a rise in the proportion of procurements tendered through it.[46] Progress has been sluggish, but not inexistent. The application of the Directive has been under constant observation, and novel funding schemes aim to further accelerate and boost the development of EDEM.

An additional field identified as crucial in boosting EDEM, and included as such in the "Defence Package" is the harmonisation of transfer rules via the Transfers Directive.[47]

2.2. Transfer rules

The Transfers Directive was created to improve EDEM by streamlining the rules and procedures regarding the cross-border transfer of defence-related products. These products are defined in the Annex of the Transfers Directive, which is regularly updated (the last update was in 2019).[48] To achieve this, the Directive introduced new licencing tools that are ultimately meant to simplify the cross-border transfer of defence-related products. The sensitive nature of these products requires licences for cross-border transfers, even within a single market. Divergent national rules on exporting defence-related products have been identified as essential factors constituting one of the major barriers to increased Europe-wide competition in this area. New tools have been developed with the expectation that they would bolster the integration of supply chains and enhance security of supply.[49]

The common licencing rules proposed by the Transfers Directive are therefore meant to tear down barriers, unify the regime of risk control and extend the benefits of the internal market to defence-related products. The Transfers Directive establishes rules on the movement of defence equipment that extend to EU Member States as well as Norway and Iceland. The new tools include general and global licencing for the transfer of defence-related products in addition to the much-utilised individual licences. The Directive also introduced rules regarding the granting of licence exemptions, which were in turn meant to be determined by national governments.[50]

Individual transfer licences allow an individual supplier to transfer a specified quantity of specific products to a single recipient in one or several shipments.[51] Any

46 Ibid., pp. 4/25, 5/25.

47 *Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community*, 2009.

48 The list of defence-related products was last updated via *Commission Delegated Directive (EU) 2023/277 of 5 October 2022 amending Directive 2009/43/EC of the European Parliament and of the Council as regards the updating of the list of defence-related products in line with the updated Common Military List of the European Union of 21 February 2022*, 2023.

49 European Parliament, 2021, para. B.

50 Article 4(2) of *the Transfers Directive*.

51 Article 7 of *the Transfers Directive*.

further attempt to make any other transfer obliges the supplier to request a new licence. The new licencing tools introduced by the Transfers Directive simplify the procedure by enabling licences to be extended to additional transfers. The so-called global transfer licences allow an individual supplier to make multiple transfers of specified products to specific recipients in one or more Member States for a period of three years, which may be renewed.[52] General transfer licences cover certain types of defence-related products, making it possible for suppliers to effectuate transfers without requiring a specific licence. Such licences may also contain specifics regarding the countries to which they are extended, details of the purpose of the transfers and information on recipients of the products.[53]

The general transfer licence constitutes the principal tool of the Transfers Directive, and its use and promotion by Member States were made mandatory. The Directive prescribes that, under certain conditions, Member States must publish general transfer licences covering situations such as when the transfer is made for the purpose of demonstration, evaluation, exhibition, or even maintenance and repair.[54] With this, Member States are basically encouraged to utilise the general transfer licence as a tool. However, Member States are at liberty to determine the types of products to which they want to extend such licences and the conditions applicable to them. In all cases, the national authorities must be notified of the first use of a general transfer licence. Recipients must obtain a certification to prove reliability and avoid misuse of licences.[55] Licences are uploaded to the Register of Certified Defence-Related Enterprises (CERTIDER), which also includes information on national contact points and general transfer licences. A quick browsing of the register reveals deficiencies in the implementation of the Transfers Directive, as demonstrated by the infrequent and scarce use of its tools.[56]

An evaluation ordered by the European Commission in 2016 revealed that there were differences in the transposition of the Transfers Directive at the level of Member States, which constituted barriers to its application. This issue is similar to the Defence DPD. At the time the evaluation was undertaken, the individual transfer licences were still favoured over general ones, despite the express purpose of the Directive to streamline transfers by replacing the former with the latter.[57] Similar to the case of DPD, the European Commission concluded that the Transfers Directive did not require amendments but rather needed clarification.[58] For this reason, the

52 Article 6 of *the Transfers Directive*.
53 Article 5 of *the Transfers Directive*.
54 Specific obligations are included in Article 5(2) of *the Transfers Directive*.
55 Article 9 of *the Transfers Directive*.
56 *The Register of the Certified Defence-related Enterprises*. [Online]. Available at: https://webgate.ec.europa.eu/certider/ (Accessed: 9 January 2024).
57 European Commission, 2016b, pp. 5–6.
58 Ibid., pp. 10–11.

European Commission subsequently published recommendations in 2016[59] and 2018[60] aiming to assist Member States in harmonising the transposition and implementation of the Directive. Unfortunately, a sneak peek of the CERTIDER suggests that these efforts have not been met with an active response from Member States.

2.3. The "Defence Package" on balance

The "Defence Package", which is aimed at boosting the internal market for defence-related products, seems to have been overridden by the internal market itself. Alternatively, they may be dominated by national interests. The need for 'a common European security and defence culture'[61] remains, and the challenges for its accomplishment appear to remain unsolved. The failings of the "Defence Package" have not been overturned, despite the apparent political agreement behind this task. The actions of Member States and industry actors seem to override the declared intent. The "Defence Package" had a difficult task from the outset. Starting with the Great Recession, there was a steady decrease in defence investment, which purportedly contributed to the renationalisation of supply chains, admittedly thwarting the objective of the "Defence Package" which was the 'de-fragmentation of markets'.[62]

The 2016 Evaluation of the Transfers Directive noted that this instrument has succeeded in creating a smaller European market for less sensitive equipment, but high-tech goods remained excluded.[63] Similarly, the 2016 report on DPD found that its objectives were only partially achieved.[64] While the presented challenges as to their implementation remain, the resolution of the European Parliament, drawing on the extensive analysis carried out on the "Defence Package", does not recommend

59 *Commission Recommendation (EU) 2016/2123 of 30 November 2016 on the harmonisation of the scope of and conditions for general transfer licences for armed forces and contracting authorities as referred to in point (a) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council*, 2016; *Commission Recommendation (EU) 2016/2124 of 30 November 2016 on the harmonisation of the scope of and conditions for general transfer licences for certified recipients as referred to in Article 9 of Directive 2009/43/EC of the European Parliament and of the Council*, 2016.

60 *Commission Recommendation (EU) 2018/2050 of 19 December 2018 on aligning the scope of and conditions for general transfer licences for the purposes of demonstration and evaluation as referred to in point (c) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Counci*, 2018; *Commission Recommendation (EU) 2018/2051 of 19 December 2018 on aligning the scope of and conditions for general transfer licences for the purposes of repair and maintenance as referred to in point (d) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council*, 2018; *Commission Recommendation (EU) 2018/2052 of 19 December 2018 on aligning the scope of and conditions for general transfer licences for the purpose of exhibition as referred to in point (c) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council*, 2018.

61 European Parliament, 2021, paras. C, D.

62 European Commission, 2016b, pp. 7–8.

63 Ibid., p. 8.

64 Cf. European Commission, 2016b, p. 5.

revision, but rather improved implementation.[65] Research in this area has revealed that DPD has improved some of the protectionist procurement practices. The modest results show a reduction in the rate of single bidding and contracts awarded without calling tenders. However, there has been a simultaneous increase in the number of contracts awarded through non-open procedures.[66]

The "Defence Package" constitutes a two-piece part of the many that complete the puzzle of the European defence equipment market. The large number of bureaucratic components in this area make it challenging to navigate without overlapping or inconsistent regulations.[67] The "Defence Package" itself very likely obfuscates the original intent of building EDEM, by containing the very means that make it possible to bypass participation in it. This is partly the reason why 'a very high volume of procurement expenditure is still incurred outside the [Defence Procurement Directive] and that an overwhelming percentage of contracts are still awarded nationally.'[68] Member States continue to protect their domestic industries and use defence procurement to continue building them. While it may serve their national economies, it creates inefficiencies in common European defence endeavours. The choice of participating in the envisaged EDEM is considered challenging for smaller Member States with less-developed industries. Without exercising protectionism as part of their acquisition strategies, it is even more unlikely that they would ever be able to develop a domestic industry capable of feeding into the supply chains of dominant companies in wealthier Member States.

The lip service paid at the EU level for the purpose of DPD to improve competition seems understandable in this economic perspective. Less developed States with smaller industry actors run the risk of their defence industries being devoured as soon as the avenues for exercising protectionism are closed. This is also demonstrated by the fact that the East–West imbalance in the defence industrial landscape has only increased with the expansion of the EU.[69] The Member States' approach, which in the defence procurement area was described as "domestic first", may imply that the consolidation of the European defence industry 'will more likely be industry-driven than policy-driven'.[70] Consolidation (also referred to in this context as "de-fragmentation") appears as rather anti-competitive, but its necessity appears logical when the aim is to cover gaps and avoid duplication in defence-related products. The fragmentation in the European defence equipment market stems not from the emancipation of competition but, rather from the tenacious grip of persisting protectionism.

Beyond pure protectionism, the deficient implementation of the Transfers Directive, despite having been transposed by all Member States for well over a decade,

65 European Parliament, 2021, paras. D, 10–11, 14.
66 Czibik et al., 2020, p. 8.
67 European Commission, 2016b, p. 9.
68 European Parliament, 2021, para. 4.
69 Briani et al., 2013, p. 34.
70 Ibid., p. 59.

also points to a lack of trust between them.[71] Wider collaboration within the EU seems more difficult to achieve, even when collaboration between three Member States is delayed by disputes over who gets to do what part.[72] This would likely mean that any incentive programme at the EU-level requiring industry consolidation (i.e. smaller industry players being left by their home states at the mercy of the market) in return for promises of a type of dispersion of production would likely be viewed with suspicion. In addition, in the broader NATO context, EU industrial actors are also required to compete with U.S. exports. A previous round of relaxing of export control measures in the United States has been decried as handing these companies a regulatory advantage, and putting them on an "unequal footing" with European companies.[73] The significant political support in the United States for defence industrial policy is closely tied to the dispersion of production and politicians' eagerness to create and maintain jobs. Emulating this at the European level would require concrete interventions or disproportionate incentives, which may clash with other interests and other EU rules.

With defence spending in decline at the beginning of the previous decade, some argued that the "Defence Package", as a demand-based policy instrument, could not be expected to have effectively reorganised the structure of EDTIB.[74] Now that a crisis has ensued, and defence spending has been ramped up, it remains to be seen whether the demand-side approach of the "Defence Package" will be able to serve its purpose. To date, there has been much scrambling by Member States, once again in an individual manner, to stock weapons from wherever they can get them. In this sense, the news appears to be split almost evenly between announcements of plans for common acquisitions and new equipment acquisitions, following *everyone for themselves* shopping spree.

3. Funding defence cooperation to overcome reluctance

The choice of directives for 2009 was carefully considered. This legal instrument allows for flexibility by granting Member States some leeway during their transposition to adapt them to national priorities. However, more than a decade after the implementation of the "Defence Package" the envisaged results have only partially been achieved. EDEM continues to be fragmented, and the challenges that were supposed to be tackled still require resolution. The directives were used only in a limited manner, thus having a limited effect on the development of EDTIB. The EU

71 European Parliament, 2021, para. 18.
72 Machi, 2022.
73 European Commission, 2016b, p. 8.
74 Mölling, 2013, pp. 2–3.

has devised a series of financial incentives to overcome Member States' reluctance to collaborate.

3.1. Funding cooperative spending

Recently, there has been much focus on cooperative spending by EU Member States, with the aim of leveraging economies of scale, covering gaps and avoiding duplications.[75] Although this is not a novel concept, it needs to be revisited, considering the reluctance of Member States to cooperate. As per the CARD Report of 2022, cooperative spending in the second CARD cycle (2021–2022) as compared to the first (2019–2020), dropped from 19% to 18% of all investments in defence programmes.[76] The percentage of collaborative defence equipment procurement of total defence equipment procurement is even lower, being at its lowest in 2020 at 11%.[77] This is contrastive from the 35% benchmark to which the EU Member States agreed to.

To reinforce EDTIB, Member States agreed on a more hands-on approach to cover the gaps. Therefore, as a consequence of Russia's invasion of Ukraine, the European Council considered it necessary to advance a budget regulatory proposal. The proposal for establishing European Defence Industry Reinforcement through the Common Procurement Act (EDIRPA) was advanced in July 2022. It aims to address 'the EU's most urgent and critical defence capability gaps and incentivise the EU Member States to procure defence products jointly'.[78] Through this, the European Council aimed to increase defence spending and make it more efficient. In a sense, this is also meant to be a response to the criticism often voiced against European members of NATO that they are heavily reliant on the United States for their security and are unwilling to increase their defence spending. The envisioned increase in spending through EDIRPA should result in more efficiency. Efficiency in this area means conducting collaborative investments in defence programmes.[79] This ensures that states receive *more bang for their buck*.

With this regulation, the EU proposed a funding scheme to encourage joint purchases, making available a budget of 300 million euros for this purpose until the end of 2025.[80] This instrument is meant to address the 'most urgent and critical defence product needs, especially those revealed or exacerbated by the response to Russian aggression against Ukraine'.[81]

75 This was a major topic already in 2016, see: European Commission, 2016a.
76 European Defence Agency, 2022a, para. 22.
77 European Defence Agency, 2022b, p. 16.
78 Clapp, 2023.
79 A priority mentioned in the 2022 EU *Strategic Compass*, as well as *the Versailles Declaration* of March 2022.
80 European Parliament, 2023; *Regulation (EU) 2023/2418 of the European Parliament and of the Council of 18 October 2023 on establishing an instrument for the reinforcement of the European defence industry through common procurement (EDIRPA)*, 2023.
81 Article 7(1)(a) of EDIRPA.

Member States that want to participate in procurement under EDIRPA must adhere to a few ground rules. Joint purchases must be made in the form of consortia involving at least three Member States. The spending scheme includes provisions akin to requirements of local content. Contractors must be established and have their executive management structures either in the EU or Iceland, Liechtenstein or Norway (the so-called associated countries). Contractors must not be subject to control by a non-associated third country or entity. Derogation under this requirement can only be permitted under strict guarantee from those who request it. Components originating in the EU and associated countries must account for at least 65% of the end-product costs. Contractors must also use facilities and resources based in the EU or an associated country, except if producers do not have the appropriate infrastructure in the prescribed locations.

The EDIRPA also sets a cap on the contribution, at 15% of the total funds made available under it, and at 20% of the estimated value of the procurement. This should allow for the distribution of funds across more projects, which, in light of the budget made available under EDIRPA and the costs associated with defence procurement in general, would otherwise run the risk of being absorbed by a single project.

As alluded to, EDIRPA may be criticised for the lack of ambition reflected in its budget. The 500 million euros envisaged in the initial proposal and the 1 billion euros proposed by the European Parliament would also have been a far cry from what is needed in this field but would have certainly been more than the 300 million euros finally agreed upon. As a pilot project, it may be appreciated for what it is attempting, which is to bring Member States closer in terms of their defence procurement priorities, bringing with it all the benefits of such cooperation: consolidation, better access to products and enhanced interoperability among allies. While its objectives of enhancing adaptation to structural change and ramping up manufacturing capacity would undoubtedly benefit EDTIB because of its budget, it is doubtful that EDIRPA will be able to accomplish them. Such doubts were also expressed by the European Economic and Social Committee (EESC), which was entrusted to provide an advisory opinion on the proposal. The EESC stated that the initiative was "rather weak" as an industrial policy instrument.[82]

To achieve the objectives of EDIRPA, the regulation mandates that the work of the Defence Joint Procurement Task Force and that of the Strategic Compass for Security and Defence be considered.[83] With an emphasis on covering urgent capability gaps, the European Commission and EDA proposed focusing on three important tasks: coordinating procurement, replacing legacy systems and reinforcing air and missile defence systems. For this purpose, they proposed establishing a Defence Joint Procurement Task Force.[84] As a result of its work, the Task Force identified a number of areas in which joint procurement should be considered: (i) medical equipment

82 EESC Opinion, 2022, paras. 1.3, 3.6.
83 Article 3(2) of the EDIRPA Regulation.
84 European Commission, 2022, pp. 7–8.

and supplies; (ii) chemical, biological, radiological and nuclear individual protection equipment; (iii) anti-tank systems and missiles; (iv) soldiers' equipment and radios; (v) ammunition, explosives, mortars and multiple launch rocket systems; (vi) missiles, air defence, man portable air defence systems and bombs; and (vii) small arms.

While these efforts are definitely welcome, EU funding and common procurement programmes such as EDIRPA bring in a new set of political challenges. It must be noted that *protectionist* conditions are not well received by allies, such as the United States. While it has been calling for an improvement in EDTIB, the United States has previously criticised efforts aimed at its exclusion from such programmes.[85] The American Chamber of Commerce also expressed similar criticism regarding EDIRPA.[86] Nevertheless, considering the number of F35 fighters recently acquired by European NATO members, EDIRPA could hardly weaken the American defence industry.

Another potential conflict may arise between political will and legal possibilities. The EU must adhere to several rules at its core. Article 41(2) TEU does not allow for the use of the common budget for 'expenditure arising from operations having military or defence implications (…).' However, where there is a will, there is a way, and a way has indeed been found. Therefore, EDIRPA was drafted on the basis of Article 173 TFEU, which sets out rules for enhancing the competitiveness of the European industry, in this case, fostering the competitiveness and efficiency of EDTIB.[87] Despite this apparent limitation, there are now several spending schemes that are active, aiming, among others, to enable defence-related research and development (R&D),[88] common procurement of defence-related products and the development of dual-use items and technologies. Off-budget collaboration is not limited to Article 41. However, other programmes must adhere to stricter rules. For this reason, EDF, which represents the replacement of the previous Athena mechanism, now focuses on promoting cooperation, as well as research and development, whereby novel equipment may only be funded up to the prototype phase.

> Beyond the more urgent tasks covered by rapid joint procurement efforts, the European Commission proposed establishing an incentive system to serve its purposes over a longer period. The European Defence Investment Programme (EDIP)[89] establishes rules for forming a European Defence Capability Consortium for joint procurement, which would benefit from VAT exemption.[90] Despite the urgency of

85 *US warns EU over "poison pill" defence plans*, 2019.
86 American Chamber of Commerce to the European Union, 2022.
87 Article 3(1)(a) of the EDIRPA Regulation.
88 This is especially important as research and development spending did not follow procurement spending in recent years. Cf. Tigner and Landriani, 2023.
89 Details of the project can be found on the EESC's webpage. [Online]. Available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/european-defence-investment-programme (Accessed: 9 January 2024); see: *European Defence Investment Programme*, no date.
90 European Commission, 2022, p. 10.

implementing such schemes, negotiations tend to drag on, which increases delays in obtaining the envisaged results.

The EU demonstrates that it is ready to go beyond its own limits, whether legal or financial, and determine ways to tackle short-term urgencies and initiate long-term plans. Such programmes aimed at harmonising Member States' defence expenditures, ramping up production and boosting innovation have mushroomed in recent years. The centre of this is the EDF. It has a budget of almost 8 billion euros, which is made available for collaborative projects in R&D during 2021–2027.[91] In 2019, a two-year programme was launched called the European Defence Industrial Development Programme, aimed at supporting competitiveness and innovation capacity in the EU's defence industry.[92] As a short-term instrument, EDIRPA is not meant for industry development but rather to facilitate procurement coordination, maximise economies of scale and avoid duplication and competition where supply is limited.[93] The EU also has institutions aimed at boosting innovation and industry development, the most important of which are the EU Defence Innovation Scheme and the Hub for EU Defence Innovation, with programmes such as Galileo targeting defence industrial development. In addition to this list, NATO's Science and Technology Organization and programmes made available via NATO's Innovation Fund and its support programme, the NATO Defence Innovation Accelerator for the North Atlantic, also support defence innovation. As a direct consequence of Russian aggression against Ukraine, the EU used the European Peace Facility (EPF), an off-budget fund, to reimburse Member States for ammunition donated to Ukraine, fund joint procurements and help ramp up production capacity.[94] The Act in Support of Ammunition Production, agreed upon in 2023, and based on Article 173 TFEU, was organised to accelerate joint procurement and deliver one million rounds of artillery ammunition to Ukraine in a year.[95] In the context of the ongoing war on its borders and going beyond the previously mentioned emergency measures, in March 2024, the European Commission unveiled its first European Defence Industrial Strategy (EDIS)[96] and proposed EDIP.[97] These are aimed at bolstering the EU's security and defence preparedness, proposing that Member States 'invest more, better, together, and European'.

Opportunities abound for companies, from startups, through SMEs, to large enterprises. While the above listing does not attempt to present an exhaustive account of all funding programmes, there are actually numerous programmes. However, funding appears to be meagre, when compared to the astronomical amounts usually

91 See: European Commission, 2021a.
92 See: *European Defence Industrial Development Programme (EDIDP)*, no date.
93 European Commission, 2022, p. 1.
94 *European Peace Facility (EPF)*, no date.
95 *Act in Support of Ammunition Production*, no date.
96 *European Defence Industrial Strategy*, no date.
97 *European Defence Industry Programme*, no date.

discussed vis-à-vis regular defence spending efforts. However, neither the number of programmes nor the amount of funding at their disposal are adequate for addressing the most severe problem faced by governments in the defence procurement area: low production capacity. While accessing existing funding opportunities has a certain duration, delays are even more significant in terms of delivering on the money that is thus spent. Consequently, after providing programmes and funding, a new challenge appeared, which was a result of the fewer number of purchases induced by years of reduced spending.

In addition to the general challenges affecting the entire economy, such as inflation and shortages in the supply of critical raw materials,[98] there is also a specific lack of capacity in terms of meeting demands for high volumes of production. As previously mentioned, the defence industry must survive for years with underfunded defence budgets. This implies that many companies have reduced their output capacities and lack the resources to meet the demands at the pace required by current events. Furthermore, complex regulatory and administrative structures are ill-prepared for the quick ramp-up in spending. An example from Germany, a country widely regarded as highly competent, illustrates how difficult this can be. Despite the unprecedented political will demonstrated when the German Chancellor announced the "Zeitenwende", and a ramp-up in military spending with a 100 billion euro special fund, the challenges to acting expeditiously in spending that money have proven too great.[99] Additionally, a special law was adopted to accelerate procurement processes.[100] Although a temporary solution, it was noted that this law reduces both transparency and competition guarantees in defence procurement and may be in violation of the EU's DPD.[101] This only serves as an example to point out a wider critique that is often placed against regulation in general, and in this case against defence procurement rules in particular, that "a more efficient" procurement regulation naturally implies compromises in the area of transparency and competition rules. Exactly the opposite of what the EU attempted through the "Defence Package". This is just a more recent iteration of the limited implementation of the EU's regulatory framework in Member States' domestic regulation, whereby a deficiency in harmonised regulatory integration effectively hinders the envisioned EU-wide cooperation.[102]

Statistics also show an increase in funds earmarked for defence spending. Less developed Member States, typically in Eastern EU, feeling more of a threat from the East, have also increased defence spending. However, another dimension of lack of capacity must be addressed: gaining access to the previously mentioned funding and development support schemes. This discrepancy was confirmed by the results of the 2021 and 2022 EDF calls for proposals.[103] This issue can be addressed in several

98 Council of the European Union, 2023.
99 Knight, 2023.
100 *Bundeswehrbeschaffungsbeschleunigungsgesetz vom 11. Juli 2022 (BGBl. I S. 1078)*, 2022.
101 See also: *A Critical Assessment of the Bundeswehr Procurement Acceleration Act*, 2022.
102 The difficulty in cooperation frustrates military officials, cf. Siebold, 2023.
103 As shown in: European Defence Fund, 2022; and in: European Defence Fund, 2023.

ways, such as the inclusion of incentives in calls for proposals, as is being done with SMEs, with consortia that include first-time participants eligible to receive extra points. In this way, more experienced companies forming consortia will be incentivised to include first-time participants, who will, in turn, gather experience for future rounds of funding. One may also envision special criteria modelled on Horizon Europe Widening, which is also aimed at boosting research and development in Central and Eastern Europe.

3.2. Focus on SMEs

A number of funding schemes expressly refer to SMEs, in an area that is dominated by big players. Their dominion appears logical, and is even necessary in a field of such high sophistication as defence manufacturing. However, the funding programmes rightly recognise the role to be played by SMEs, and it fits into the discourse, which states that 'it is hard to develop new things in big organisations', and that '[n]ew technology tends to come from new ventures – startups'.[104]

Defence procurement disproportionately favours large players, with data suggesting that SMEs are less successful in winning contracts under DPD than under general EU public procurement.[105] SMEs tend to be increasingly nimble and creative, and hold much potential for innovation. However, weapons systems and, consequently, the defence industry have become highly complex, making it difficult for smaller players to participate. At this level of sophistication, it is difficult for a smaller company to produce a stand-alone product. The defence industry in general, and SMEs in particular, find it challenging to attract financing from private sources. It is recognised that SMEs hold significant potential for innovation, but it also turns out that around 80% of R&D projects fail.[106] This renders such projects highly risky to investors. Further disincentives for private financing come from other EU regulatory priorities such as green financing rules and the application of Environmental, Social and Governance criteria.[107] The cumbrance represented by having to comply with such regulation, may seriously affect the willingness of private sector funds to invest in the defence industry.

Beyond R&D for innovation, one of the methods for SMEs to thrive is to latch on to the manufacturing stream of an original equipment manufacturer and become a sub-supplier. According to research conducted by the European Commission, there are around 2,500 SMEs in the EU 'operating in the multi-layered and often transborder defence supply chains'. These SMEs 'serve the land (39.6%), air (30.5%), maritime (18.7%), cyber (7.8%), and space (3.4%) defence domain customers'.[108]

104 Thiel and Masters, 2014, p. 10.
105 European Parliament, 2021, para. 28.
106 Maulny et al., 2023, p. 3.
107 European Defence Agency, 2023, paras. 13–14. See also: Maulny et al., 2023, pp. 3–5.
108 European Commission, 2022, p. 5, n. 17.

However, subcontracting is difficult, and obtaining certification incurs increased costs.[109] In breaking down "disproportionate and unfair disadvantages", some States have moved towards solutions, by adopting public policy tools to facilitate SMEs' access to public defence and security contracts.[110] Funding programmes may also incentivise innovation and SME participation.[111]

Recognising the inherent disadvantages affecting SMEs in the defence sector, EU funding programmes concentrate on providing smaller companies with more opportunities. There was no lack of willingness to participate. The EDF programmes were highly sought after in 2023, with good uptake in programmes targeting SMEs.[112] The consortia formed to access EDF funds may also cascade such funds to SMEs and startups. In the case of EDIRPA, the call incentivises procurement of equipment, the manufacturing of which takes place with the participation of SMEs or mid-caps. Furthermore, EDF offers business coaching to SMEs for two years, providing guidance on overcoming business challenges and reducing the time from research to development or from development to the market. Despite these efforts, SMEs receive only 20% of actual funding.[113]

Considering that security of supply concerns have led procurers to focus on equipment that can be obtained from national sources, SMEs find themselves in an even more difficult situation when it comes to breaking outside their home markets. Accordingly, the European Commission published a set of proposals to enhance cross-border market access for SMEs.[114] However, SMEs are best served by finding new market sectors. This may be the reason why many SMEs tend to gravitate towards the area of dual-use items, which enables them to extend their clientele beyond the narrower defence sector. This presents additional challenges, as synergies between civilian and military products may result in vulnerability in the supply chain. In a field where security of supply is a tantamount objective, industry players must be aware of their supply chains and solve possible dependencies before they pose a problem.

Focusing on dual-use items may also provide companies with more avenues to obtain financing from public sources. The European Commission acknowledged this opportunity when it launched public consultations via a recently published white paper aimed at exploring opportunities to shift resources to support R&D of technologies with dual-use potential.[115] Dual-use projects may benefit from European

109 European Parliament, 2021, paras. H–J.
110 Masson and Martin, 2015, pp. 38–39.
111 Greenacre, 2023.
112 Record high number of proposals received in the 2023 round of the European Defence Fund; Defence Industry Europe, 2023.
113 See statistics in: European Defence Fund, 2022; and in: European Defence Fund, 2023.
114 *Commission Recommendation (EU) 2018/624 of 20 April 2018 on cross-border market access for sub-suppliers and SMEs in the defence sector*, 2018.
115 European Commission, 2024. Previously, the Commission also published the Action Plan on Synergies between Civil, Defence and Space Industries, see: European Commission, 2021b.

Investment Bank (EIB) financing.[116] Such financing could be tied into the EIB's aim to finance 'projects for developing less-developed regions', as per Article 309(a) TFEU. Several Member States have called on EIB to invest in core defence projects, but this would require an amendment to its rules.[117] Further funding opportunities lie in instruments such as the Important Projects of Common European Interest or CASSINI, which may be appropriate for financing the R&D of dual-use technologies.

A comprehensive empirical study may reveal how much funding programmes have accomplished in their quest to de-fragment defence markets and how much space they have actually created for SMEs. Additional questions regarding the possibility of circumventing the conditions for accessing funding opportunities should be explored. For now, it appears that protectionist practices in defence procurement are paradoxically maintaining fragmentation in the defence industry and providing many SMEs the lifeline they need to survive in this market. It is possible that without States' willingness to support their domestic defence industry, SMEs would not have much of a chance in the face of market competition.

4. Protectionist procurement – Offsets trending

States often turn to different techniques to ensure that the bidder they favour wins a particular tender. Such practices include the direct awarding of contracts, the organisation of by-invitation-only bids (thus avoiding competition) or even the tailoring of tender specifications in a manner that severely narrows the competition. The limited use of TED, as previously mentioned in the context of DPD, and the generally-restricted circulation of advertisements, also serves to exclude some bidders. The defence sector is markedly secretive; however, these techniques are generally regarded as manifestations of corruption.[118] However, in the field of defence procurement, the corruption and anti-corruption rhetoric seldom emerges.[119] The preferred term is protectionism. This has more to do with the specifics of the defence industry's ownership structure than anything else. State ownership in the defence sector's national champions is an important driver of such *protectionism*.[120]

As previously mentioned, a factor that is highly valued in defence procurement is the security of supply, in terms of inputs related to a country's defence capabilities. Securing predictability in the supply chain is an important driver of the ongoing recalibration of international trade and investment regimes. While the trend

116 As also noted in: European Commission, 2017a.
117 Foy, 2024.
118 Cf. World Bank Group, 2010, p. 7.
119 Although it is not completely lacking, cf. OECD, 2016, p. 3.
120 Czibik et al., 2020, p. 5.

in the general economy towards re-shoring and friend-shoring is a consequence of securitisation occurring in more areas of the economy in the defence sector, this is not a novel topic. Beyond friend-shoring, security of supply may be considered optimal when the production of inputs moves within the borders of the procurer state. Therefore, controlling the means of production is essential. Therefore, the market logic of obtaining *the best value for the money* is given a new dimension and attracting suppliers into offset arrangements and joint venture agreements may receive priority. Procurer states use these tools to attract investments and link autochthonous companies to supply chains through local content requirements. Such practices may not be compatible with short-term or urgent procurement plans because they tend to slow down the process. However, they are quite adequate for the long-term plan of building up the domestic defence industry, often with the participation of the state as part-owners.[121]

Experts describe a strong defence industry as characterised by the presence of a 'large number of privately-owned firms, free entry to the market and competitively determined fixed-price contracts', where 'profits attract new entrants and losses lead to exits'. They contrast this with what would be considered as a weak defence industry, which is one that is 'characterised by state-owned firms, subsidies, protectionism, and cost-plus contracts'.[122] Considering the extensive use of offsets, it is difficult to apply market logic fully to defence procurement.

A generic term, mostly familiar to experts in the field of public procurement, an *offset* is a form of compensatory procurement requirement, formulated to offset the expenses associated with acquiring defence equipment in favour of the domestic economy of the procurer.[123] This often takes the form of a return commitment from a supplier to engage in industrial cooperation. A simple perspective is that offsets are basically 'those goods and services on which a government chooses to place [this] label'.[124]

Offsetting has become a major component of the defence procurement policy aimed primarily at promoting the development of the procurer's national defence industry. Offsets typically appear in two forms: direct and indirect.[125] Direct offsets are contracts that directly tie into procured defence products. For example, acquiring helicopters may come with an obligation to set up servicing work or production of components within the procuring country. Through this, a country not only acquires equipment, but also creates jobs, develops competence and arranges for the transfer of technology related to the acquired equipment. Indirect offsets involve bundling the procurement deal with an incentive that is completely unrelated to the acquired products. In this regard, the acquisition of helicopters from a particular supplier may

121 Cf. Schroeder et al., 2020.
122 Hartley, 2013, pp. 4–5.
123 Cf. Csécsy et al., 2015, pp. 29–30.
124 For more definitions, see: Ungaro, 2013, pp. 4–5.
125 Cf. Martin, 1996, p. 3.

be part of a larger deal to establish handgun production in a procurer's country. Furthermore, scholars distinguish between three categories of offsets: countertrade, whereby the seller purchases goods and services from the buyer's territory; local content requirement, involving a commitment to the source part of the contract from the buyer's territory; and the bundling of requirements, whereby the buyer conditions its purchase on the provision of other products or services.[126] Of these three categories, the local content requirement presents the most interest, as it often takes the form of establishing facilities through foreign direct investment, joint ventures and co-production arrangements. Economists consider these to be the most advantageous types of offsets.[127] Joint ventures are usually long-term agreements that aim to build defence and industrial capabilities within a country. Such agreements usually involve four actors: manufacturer, manufacturer's government, contracting government agencies and local defence champion.[128]

The scale of investment resulting from the offset agreement depends on two major factors. On the one hand, the offer of the procurer states its financial capacity and what it is able to offer in terms of a specialist workforce and infrastructure. However, there may be significant restrictions on how much intellectual property, technology and the home state of an original equipment manufacturer allow it to share. Without delving into further details on these aspects, it may be concluded that investments pursuant to offsets are limited on these fronts; consequently, such arrangements range from servicing to component manufacturing and supply, through final assembly, to licenced production and full domestic production of a weapons system. Therefore, governments must be realistic about the market potential of compensatory arrangements and pay attention to the selling potential of a particular product. They must also be realistic about their own capacities and settle for producing a component instead of attempting to operate a full weapons system plant if they lack experience. However, these business considerations require detailed planning and time-consuming negotiations.[129]

Viewed in its entirety, it should be easily understood why procurer states perceive so much advantage in obtaining at least some form of offset. It then becomes evident why they use existing loopholes and disregard the EU's insistence on the application of market logic. The offsets are useful in various settings. They may help with the political justifications for military spending. They are also an efficient means to building long-term relationships between the procurer and the supplier or supplier's home State. For States, it is a tool for ensuring security of supply by localising military industrial production. For companies, it is a way to ensure that they win major supply contracts. These are some of the factors that fuel enduring

126 Markowski, Hall and Wylie, 2010, pp. 139–140.
127 Martin, 1996, pp. 24–25.
128 Schroeder et al., 2020, p. 3.
129 Detailed analysis of a major procurement contract implicating detailed offset requirements is contained in: Seguin, 2007.

support for these arrangements.[130] The creation of jobs may be a good justification for increasing defence spending, but the development of an advanced defence technological and industrial base is necessary to gain the ability to absorb and maintain complex military equipment manufacturing potential.[131]

Although these practices distort competition, the reasons presented above make a compelling case as to why less-developed Member States, especially, will likely continue to use offsets. As a matter of policy, France and Germany do not allow offsets. However, they can afford such policies as they dispose of mature defence industries. Large actors in the defence industry also work together on several successful projects.[132] This perpetuates underdevelopment in the defence industries of Member States on the periphery. The room for manoeuvre of these Member States is further limited by the fact that legislation and policy requiring offsets more generally are considered to be in violation of EU law by the European Commission.[133] The DPD does not mention offsets expressly; however, circumscribing them forbids such practices. However, this extends only to offsets in the indirect form. Direct offsets are nevertheless possible when the exemption under Article 346 TFEU is used in a justified manner during a particular procurement, that is, the exemption is necessary and proportional. It must be highlighted though, that the offset itself must also be justified under Article 346 TFEU exception.[134] Furthermore, direct offsets involving R&D are expressly carved out of DPD.[135] In terms of EU law, offset requirements may violate the fundamental freedoms and basic principles laid down in treaties. Specifically, offsets may violate the freedom of establishment, free movement of goods and services, principles of equal treatment, non-discrimination and transparency. Therefore, they are considered incompatible with the Treaty and DPD. This viewpoint was clarified by the European Commission's Directorate General for Internal Markets in its Guidance Note on Offsets, which, while non-binding, cautions procurer Member States that the use of offsets may constitute an infringement of the Treaty.[136] The Commission also took action on this basis, launching infringement procedures against trespassing Member States while also looking to dissuade others from using offsets.[137] Despite EU opposition, offsets continue to be in use. As noted in a research paper published in 2015, '[p]olicies to reform offsets remain purely cosmetic.'[138] A 2016 report of the European Commission concluded that offsets were

130 Jovovic, Strang and White, 2021.
131 Ibid.
132 *Britain, Japan and Italy sign advanced fighter jet programme treaty*, 2023; Meier, 2017.
133 Directorate General for Internal Markets and Services, 2016, paras. 21, 26.
134 Ibid., para. 23.
135 Recitals 34, 55 of *the Defence Procurement Directive*.
136 Directorate General for Internal Markets and Services, 2016, in particular para. 26.
137 European Commission, 2018.
138 Masson and Martin, 2015, p. 40.

in use and their frequency only "marginally decreased".[139] This is also confirmed by the annual report to Congress on offsets in the defence trade prepared by the Bureau of Industry and Security of the U.S. Department of Commerce.[140]

It must also be highlighted that the continued application of protectionist procurement policy has had a lasting effect on the fragmentation experienced in the European defence industry. EDTIB already has numerous gaps and duplication of capabilities.[141] While cooperative procurement has many advantages, it seems unable to outcompete the advantages that states see in protectionist procurement. One may argue that synchronising procurement efforts at the EU or NATO level, considering their size and divergence in their members' interests, is more difficult. The current crisis also reveals acute differences in the threat perceptions of NATO members.[142] Even in smaller alliances, such as the Nordic Defence Cooperation, where a convergence of interests may appear easier to achieve, efforts to synchronise defence procurement and industrial development have yielded limited results.[143]

Protectionist procurement generally contributes to major distortions in the defence sector. Therefore, it is questionable whether many European defence companies would be able to compete under regular rules. Defence companies benefitting from "close relations with national governments" is a matter that the European Commission drew attention to in a document proposing solutions that drive efficiency in cooperative procurement.[144] However, clinging to the application of free-market principles and regular competition policies may not be a way towards bolstering EDTIB. However, the tools used thus far have not had a significant effect. Operating the defence industrial development according to market logic would also have a small number of *winners*, possibly leaving numerous Member States dissatisfied. Such a policy would surely be advantageous for Member States with strong defence industries. In such cases, pushing for a more market-based approach to defence procurement would see large companies expand further, swallowing up smaller players. Expanding protectionism to the European level would, in turn, serve to exclude successful U.S. and South Korean companies, which have proven to be relatively competitive at this time of crisis. Many Member States, especially those that are increasingly threatened by their proximity to Russia, may not be best served by such a protectionist approach to open strategic autonomy. Their continued reliance on the United States has been reiterated from time to time, among others, through

139 *Report from the Commission to the European Parliament and the Council on the implementation of Directive 2009/81/EC on public procurement in the fields of defence and security, to comply with Article 73(2) of that Directive*, 2016, p. 5.

140 U.S. Department of Commerce, 2023.

141 European Commission, 2017b, p. 8.

142 In a recent survey conducted in several European countries with elections in 2024, the question regarding issues that changed peoples' views of the future, shows a definite divide in terms of countries' proximity to Russia. Cf. Krastev and Leonard, 2024.

143 Dahl, 2021, pp. 174–175.

144 European Commission, 2022, p. 5.

the acquisition of defence-related equipment. Prioritising defence cooperation in the NATO framework, as opposed to other European frameworks of collaboration, has always been a priority for these EU Member States. This was also demonstrated by Poland's participation in PESCO, which from the start was conditioned on the primacy of NATO planning.[145]

5. Concluding remarks

In consonance with the case of a collectivised economy with which many Central and Eastern European countries have had extensive experience, collectivised defence and security attract a degree of free-riding and passive attitudes similar to those provoked by *non-ownership*. Structures built for collective action have often failed to deliver more cooperation on defence despite their expressly-stated roles. These organisations must nudge their passive members towards more action and more efficient cooperation. The promise to meet the 2% spending on defence agreed upon at the 2014 NATO Summit in Wales should be met by 2024. Although increased spending is welcome, there is not enough cooperation amongst EU Member States.[146]

Collective defence planning was considered essential in the early days of NATO and was part of its first ever Strategic Concept published in 1949.[147] The EU has since placed more emphasis on it than its Member States. This also placed the EU on collision course with U.S. interests. EU–NATO and EU–U.S. relations represent additional dimensions to this complex web of interest.[148] 'We will stay transatlantic and become more European', was the promise of Ursula von der Leyen during her candidacy.[149] The United States has not been shy about voicing its criticism of the collaborative approaches to defence spending envisaged by the EU, fearing the potential effects of cutting out U.S. companies from spending schemes.[150] As revealed by a former chief executive of EDA, the United States 'aggressively lobbied against Europeans' efforts to develop their defence industrial and technological base'.[151] However, a strong EDTIB would serve United States interests as much as it would serve European interests, potentially freeing up the much-needed United States resources to focus on other priorities. Consultations on the matter via the new administrative arrangement between the U.S. Department of Defense and the EDA may bring

145 Cf. Meier, 2017.
146 Monaghan, 2023.
147 Under "Cooperative Measures" in Section 8 of the 1949 NATO Strategic Concept.
148 As also noted by Miszlivetz, 2023, pp. 161–163.
149 von der Leyen, 2018, p. 19.
150 Emmott, 2019.
151 Witney, 2019, p. 3.

about actual results in bridging the gap.[152] Enhancing Trans-Atlantic cooperation is critical, especially at this time, when, in addition to the military, academics[153] and politicians[154] are also calling for switching to a war economy in Europe. However, it is also crucial that decision makers ensure that building up EDTIB would be done in an equitable manner.

The EU has attempted to introduce market logic to defence procurement, but this would leave Member States with less-developed industries at risk of dismantling their defence industries. Maintaining competitive rules in the defence sector to ensure "fair competition" cannot be an end in itself. The end game must have a better defence industry, improved EDTIB and a capable defence force. However, additional factors such as development and cohesion should not be overlooked. Clinging to the classic principles of competition may not always be conducive to this; it may not be the best means for accomplishing the end game. This is also a thinking in the old paradigm of free trade: being more efficient, cutting costs and producing better and cheaper products would ultimately leave Europe's middle-income economies with difficulty.

The crisis now unfolding in Ukraine has presented an opportunity for the EU to step up in the area of defence industrial cooperation and deliver on its promises of cohesion. The EU missed its chance, and this is probably best demonstrated by news of various defence acquisitions. Member States filled gaps in their defence equipment requirements through off-the-shelf purchases, despite the CARD warning that such actions would further fragment and weaken EDTIB. The urgency of the situation served as a cover for the use of old, ingrained protectionist procurement methods.[155]

At the Heritage Foundation in Washington D.C. on 31 January 2024, NATO Secretary-General Jens Stoltenberg pointed out "some serious weaknesses" and gaps in the production capacity of NATO members. He highlighted the advantages of economies of scale and that NATO has an open defence market, which is advantageous to the United States. However, all NATO members should experience these advantages. Currently, the EU efforts to build up the EDTIB appear to be protectionist, and the U.S. Buy American Act has similar effects. In addition, without concrete policies aimed at bringing the advantages of this "open market" to less developed members, these members will continue to use offsets, and engage in protectionism.

Economic interests of Member States must align with defence priorities for EU-wide defence cooperation to be integrated in a legislative framework that is conducive to defence industrial development. EU defence industrial policies must

152 The text of *the Administrative Arrangement* signed on 26 April 2023. [Online]. Available on the website of the European Defence Agency: https://eda.europa.eu/docs/default-source/documents/signed-aa-eda-us-dod-2023-04-26.pdf (Accessed: 15 January 2024). See also: European Defence Agency, 2023.

153 VoxEurop, 2023.

154 Bezat, Pietralunga and Vincent, 2023.

155 Bedi, 2023.

focus on the fair and equitable distribution of such developments. For less-developed Member States, it may be better to maintain open markets in the EU and not be coerced into an exclusively European protectionist market dominated by EU players, as such an arrangement runs the risk of locking in existing inequalities.

Despite the apparent willingness of EU Member States to work together on defence, collective agreements regarding cooperation in spending or R&D have proven to be nothing more than hypocrisy. Member States' governments continue to pursue protectionism and favouritism in the area of defence; they may be right in doing so.

References

American Chamber of Commerce to the European Union (2022) 'European Defence Industry Reinforcement through Common Procurement Act (EDIPRA)', 24 October. [Online]. Available at: https://www.amchameu.eu/system/files/position_papers/european_defence_industry_reinforcement_through_common_procurement_act_edirpa.pdf (Accessed: 21 December 2023).

Bedi, R. (2023) 'Why Military Procurement Has Rarely Adhered to Authorised Schedules', *The Wire*, 9 February 2023. [Online]. Available at: https://thewire.in/security/military-procurement-authorised-schedules (Accessed: 24 November 2023).

Bezat, J.-M., Pietralunga, C., Vincent, E. (2023) ''We are now in a wartime economy', says France's top military procurement official', *Le Monde*, 15 March 2023. [Online]. Available at: https://www.lemonde.fr/en/international/article/2023/03/15/we-are-now-in-a-wartime-economy-says-france-s-top-military-procurement-official_6019480_4.html (Accessed: 25 January 2024).

European Parliament, Directorate-General for External Policies (2013) *The Development of a European Defence Technological and Industrial Base (EDTIB)*. Luxemburg: Publication Office; https://doi.org/10.2861/15836. Authored by: Briani, V., Marrone, A., Mölling, C., Valasek, T.

Britz, M. (2023) 'European Defence Policy: Between Flexible Integration and a Defence Union' in Bakardjieva Engelbrekt, A., Ekman, P., Michalski, A., Oxelheim, L. (eds.) *The EU Between Federal Union and Flexible Integration*. Cham: Palgrave Macmillan, Springer; pp. 215–238; https://doi.org/10.1007/978-3-031-22397-6_9.

Bundeswehrbeschaffungsbeschleunigungsgesetz vom 11. Juli 2022 (BGBl. I S. 1078) (2022) 11 July. [Online]. Available at: https://www.gesetze-im-internet.de/bwbbg/BJNR107800022.html (Accessed: 24 November 2023).

EPRS, European Parliamentary Research Service, Clapp, S. (2023) 'European defence industry reinforcement through common procurement act (EDIRPA)' PE 739.294, November 2023. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739294/EPRS_BRI(2023)739294_EN.pdf (Accessed: 20 December 2023).

Commission Delegated Directive (EU) 2023/277 of 5 October 2022 amending Directive 2009/43/EC of the European Parliament and of the Council as regards the updating of the list of defence-related products in line with the updated Common Military List of the European Union of 21 February 2022 (2023) OJ L 42, 10 February 2023. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023L0277 (Accessed: 24 November 2023).

Commission Recommendation (EU) 2016/2123 of 30 November 2016 on the harmonisation of the scope of and conditions for general transfer licences for armed forces and contracting authorities as referred to in point (a) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council (2016) OJ L 329/101, 3 December 2016. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016H2123 (Accessed: 24 November 2023).

Commission Recommendation (EU) 2016/2124 of 30 November 2016 on the harmonisation of the scope of and conditions for general transfer licences for certified recipients as referred to in Article 9 of Directive 2009/43/EC of the European Parliament and of the Council (2016) OJ L 329/105, 3 December 2016. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016H2124 (Accessed: 21 December 2023).

Commission Recommendation (EU) 2018/624 of 20 April 2018 on cross-border market access for sub-suppliers and SMEs in the defence sector (2018) OJ L 102, 23 April 2018. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0624 (Accessed: 2 November 2023).

Commission Recommendation (EU) 2018/2050 of 19 December 2018 on aligning the scope of and conditions for general transfer licences for the purposes of demonstration and evaluation as referred to in point (c) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council (2018) OJ L 327/98, 21 December 2018. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H2050 (Accessed: 4 November 2023).

Commission Recommendation (EU) 2018/2051 of 19 December 2018 on aligning the scope of and conditions for general transfer licences for the purposes of repair and maintenance as referred to in point (d) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council (2018) OJ L 327/94, 21 December 2018. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H2051 (Accessed: 14 November 2023).

Commission Recommendation (EU) 2018/2052 of 19 December 2018 on aligning the scope of and conditions for general transfer licences for the purpose of exhibition as referred to in point (c) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council (2018) OJ L 327, 21 December 2018. [Online]. Available at: https://eur-lex.europa.eu/eli/reco/2018/2052/oj (Accessed: 12 November 2023).

Council of the European Union (2008) 'Extract of the Council Decision 255/58 of 15 April 1958' *Legislative Acts and Other Instruments*, 14538/4/08 REV 4, 26 November. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST%2014538%20 2008%20REV%204/EN/pdf (Accessed: 7 November 2023).

Council of the European Union (2023) 'Council and Parliament strike provisional deal to reinforce the supply of critical raw materials' *Press Release*, 13 November. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/11/13/council-and-parliament-strike-provisional-deal-to-reinforce-the-supply-of-critical-raw-materials/ (Accessed: 20 November 2023).

Csécsy, Gy., Fézer, T., Hajnal, Zs., Károlyi, G., Petkó, M., Törő, E., Zoványi, N. (2015) *Ügyletek a Kereskedelmi Jogban* [Transactions in Commercial Law]. Debrecen: Debreceni Egyetem.

Csiki Varga, T. (2024) 'Opportunities for the 2024 Hungarian EU Presidency in the European Security and Defence Policy Framework' in Navracsics, T., Tárnok, B. (eds.) *The 2024 Hungarian EU Presidency*. Budapest: Ludovika University Press.

Czibik, Á., Fazekas, M., Hernandez Sanchez, A., Wachs, J. (2020) 'State Capture and Defence Procurement in the EU', *Government Transparency Institute*, Working paper series: GTI-R/2020:03. [Online]. Available at: https://www.govtransparency.eu/wp-content/uploads/2020/11/Czibik_Fazekas_H-Sanchez_Wachs_State-Capture-and-Defence-Procurement-in-the-EU.pdf (Accessed: 24 November 2023).

Dahl, A.-S. (2021) 'Back to the Future: Nordefco's First Decade and Prospects for the Next', *Scandinavian Journal of Military Studies*, 4(1), pp. 172–182; https://doi.org/10.31374/sjms.85.

Defence Industry Europe (2023) 'Record high number of proposals received in the 2023 round of the European Defence Fund' *Press Release*, 24 November. [Online]. Available at: https://defence-industry.eu/record-high-number-of-proposals-received-in-the-2023-round-of-the-european-defence-fund/ (Accessed: 17 January 2024).

Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC (2009) OJ L 216, 20 August 2009. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0081 (Accessed: 14 November 2023).

Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community (2009) OJ L 146, 10 June 2009. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0043 (Accessed: 14 November 2023).

Directive 2009/43/EC, Annex, List of the defence-related products. [Online]. Available at: https://webgate.ec.europa.eu/certider/public/defenceProductList (Accessed: 9 January 2024).

Directorate-General for External Policies of the Union (2013) 'The development of a European Defence Technological and Industrial Base (EDTIB)' *EXPO/B/SEDE/2012/20*, 10 June. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433838/EXPO-SEDE_ET%282013%29433838_EN.pdf (Accessed: 14 November 2023).

Directorate General for Internal Markets and Services (2016) 'Guidance Note, Offsets' Ref. Ares(2016)765159, 12 February. [Online]. Available at: https://ec.europa.eu/docsroom/documents/15413/attachments/1/translations/ (Accessed: 22 November 2023).

Emmott, R. (2019) 'Pentagon warns EU against blocking US companies from defence pact', *Reuters*, 14 May 2019. [Online]. Available at: https://www.reuters.com/article/markets/pentagon-warns-eu-against-blocking-us-companies-from-defence-pact-idUSL5N22Q5YQ/?_x_tr_sl=en&_x_tr_tl=pl&_x_tr_hl=pl&_x_tr_pto=sc (Accessed: 14 November 2023).

European Commission (2006) 'Interpretative Communication on the application of Article 296 of the Treaty in the field of defence procurement' COM(2006) 779 final, Brussels, 7 December. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52006DC0779 (Accessed: 14 November 2023).

European Commission (2012) 'Report from the Commission to the European Parliament and the Council on transposition of directive 2009/81/EC on Defence and Security Procurement' COM(2012) 565 final, Brussels, 2 October. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012DC0565 (Accessed: 14 November 2023).

European Commission (2016a) 'European Defence Action Plan' COM(2016) 950 final, Brussels, 30 November. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4088 (Accessed: 12 November 2023).

European Commission (2016b) 'Evaluation of Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community' COM(2016) 760 final, Brussels, 30 November. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:760:FIN (Accessed: 12 November 2023).

European Commission (2017a) 'Communication Launching the European Defence Fund' COM(2017) 295 final, Brussels, 7 June. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0295 (Accessed: 14 November 2023).

European Commission (2017b) 'Reflection Paper on the Future of European Defence' COM(2017) 315 final, Brussels, 7 June. [Online]. Available at: https://commission.europa.eu/publications/reflection-paper-future-european-defence_en (Accessed: 14 November 2023).

European Commission (2018) 'Defence procurement: Commission opens infringement procedures against 5 Member States' *Press Release*, Brussels, 25 January. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_357 (Accessed: 14 November 2023).

European Commission (2021a) 'Fact Sheet – European Defence Fund', 30 June. [Online]. Available at: https://defence-industry-space.ec.europa.eu/document/download/69aa3194-4361-48a5-807b-1a2635b91fe8_en?filename=DEFIS%20_%20EDF%20Factsheet%20_%2030%20June%202021.pdf (Accessed: 27 January 2024).

European Commission (2021b) 'Action Plan on Synergies between Civil, Defence and Space Industries' COM(2021) 70 final, Brussels, 22 February. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0070 (Accessed: 30 November 2023).

European Commission (2022) 'Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the Defence Investment Gaps Analysis and Way Forward' JOIN(2022) 24 final, Brussels, 18 May. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022JC0024 (Accessed: 30 November 2023).

European Commission (2024) 'White Paper On options for enhancing support for research and development involving technologies with dual-use potential' COM(2024) 27 final, Brussels, 24 January. [Online]. Available at: https://research-and-innovation.ec.europa.eu/document/download/7ae11ca9-9ff5-4d0f-a097-86a719ed6892_en (Accessed: 25 January 2024).

European Defence Agency (2022a) 'Coordinated Annual Review on Defence Report', 16 November. [Online]. Available at: https://eda.europa.eu/docs/default-source/eda-publications/2022-card-report.pdf (Accessed: 24 November 2023).

European Defence Agency (2022b) 'Defence Data 2020–2021 – Key findings and analysis' *Publications Office of the European Union*. [Online]. Available at: https://eda.europa.eu/docs/default-source/brochures/eda---defence-data-2021---web---final.pdf (Accessed: 24 November 2023).

European Defence Agency (2023) 'Joint Statement of EDA Steering Board: Strengthening the EDTIB's access to finance and its ability to contribute to peace, stability, and sustainability in Europe' *EDA Steering Board: Joint Statement*, 14 November. [Online]. Available at: https://eda.europa.eu/docs/default-source/news/20231114_jointstatement_accesstofinance.pdf (Accessed: 24 November 2023).

European Defence Fund (2022) 'Factsheet for 2021'. [Online]. Available at: https://defence-industry-space.ec.europa.eu/funding-and-grants/calls-proposals/european-defence-fund-2021-calls-proposals-results_en#summary-of-edf-2021-selected-projects---factsheet (Accessed: 24 November 2023).

European Defence Fund (2023) 'Factsheet for 2022'. [Online]. Available at: https://defence-industry-space.ec.europa.eu/funding-and-grants/calls-proposals/result-edf-2022-calls-proposals_en (Accessed: 24 November 2023).

European External Action Service (2016) 'A Global Strategy for the European Union's Foreign and Security Policy: Shared Vision, Common Action: A Stronger Europe' *European Union Global Strategy*, 2 June, pp. 20–45. [Online]. Available at: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (Accessed: 8 January 2024).

European Parliament (2021) 'Resolution of 25 March 2021 on the Implementation of Directive 2009/81/EC, concerning procurement in the fields of defence and security, and of Directive 2009/43/EC, concerning the transfer of defence-related products' OJ C 494/54, 8 December. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021IP0102 (Accessed: 19 November 2023).

European Parliament (2023) 'MEPs vote to strengthen EU defence industry through common procurement' *Press Release*, 12 Septmeber. [Online]. Available at: https://www.europarl.europa.eu/news/en/press-room/20230911IPR04908/meps-vote-to-strengthen-eu-defence-industry-through-common-procurement (Accessed: 20 November 2023).

EESC Opinion (2022) 'European Defence Industry Reinforcement Through Common Procurement Act', 21 September. [Online]. Available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/european-defence-industry-reinforcement-through-common-procurement-act (Accessed: 21 December 2023).

Friton, P., Wolters, C., Andree, N. (2020) 'Cooperation in Defence and Security Procurement among EU Member States: Applicable Law and Legal Protection', *European Procurement and Public Private Partnership Law Review*, 15(1), pp. 24–41; https://doi.org/10.21552/epppl/2020/1/6.

Greenacre, M. (2023) '€300M in new funding for common defence procurement aims to help SMEs', *ScienceBusiness*, 7 November 2023. [Online]. Available at: https://sciencebusiness.net/news/european-defence-fund/eu300m-new-funding-common-defence-procurement-aims-help-smes (Accessed: 17 January 2024).

Hartley, K. (2013) 'Europe's Defence Industry: An Economic Perspective' in Masson, H. (ed.) *Defining the European Defence Technological and Industrial Base: Debates & Dilemmas (I)*. Fondation pour la Recherche Stratégique. Note No. 23/13. [Online]. Available at: https://www.frstrategie.org/sites/default/files/documents/publications/notes/2013/201323.pdf (Accessed: 17 November 2023).

Hartley, K. (2013) 'Europe's Defence Industry: An Economic Perspective' in Masson, H. (ed.) *Defining the European Defence Technological and Industrial Base: Debates & Dilemmas* (I). Fondation pour la Recherche Stratégique, pp. 4–5. [Online]. Available at: https://www.frstrategie.org/sites/default/files/documents/publications/notes/2013/201323.pdf (Accessed: 14 November 2023).

Foy, H. (2024) 'Should the EIB be funding Europe's defence industry?', *Financial Times*, 8 February 2024. [Online]. Available at: https://www.ft.com/content/2d97053b-8594-44d1-96d4-269e2907a323 (Accessed: 9 February 2024).

Jovovic, A., Strang, A., White, R. (2021) 'Defense Offsets Expectations are Considerable, but Implementation is Uneven', *Perspectives*, *Avascent*, 23 February 2021. [Online]. Available at: https://www.avascent.com/news-insights/perspectives/defense-offsets-expectations-are-considerable-but-implementation-is-uneven/ (Accessed: 4 January 2024).

Knight, B. (2023) 'What happened to the German military's €100 billion fund?', *Deutsche Welle*, 28 February 2023. [Online]. Available at: https://www.dw.com/en/what-happened-to-the-german-militarys-100-billion-fund/a-64846571 (Accessed: 14 November 2023).

Krastev, I., Leonard, M. (2024) 'A crisis of one's own: The politics of trauma in Europe's election year', *European Council on Foreign Relations*, 17 January 2024. [Online]. Available at: https://ecfr.eu/publication/a-crisis-of-ones-own-the-politics-of-trauma-in-europes-election-year/ (Accessed: 15 February 2024).

von der Leyen, U. (2018) 'A Union that Strives for More. My Agenda for Europe.', *Political Guidelines for the Next Commission 2019-2024*, Publications Office. [Online]. Available at: https://commission.europa.eu/system/files/2020-04/political-guidelines-next-commission_en_0.pdf (Accessed: 21 January 2024).

Machi, V. (2022) 'Dassault chief confirms fighter prototype delay amid workshare dispute', *DefenseNews*, 21 July 2022. [Online]. Available at: https://www.defensenews.com/global/europe/2022/07/21/dassault-chief-confirms-fighter-prototype-delay-amid-workshare-dispute/ (Accessed: 14 November 2023).

Markowski, S., Hall, P., Wylie, R. (2010) 'Buyer-seller interaction in defense procurement' in Markowski, S., Hall, P., Wylie, R. (eds.) *Defence Procurement and Industry Policy – A small country perspective*. 1st edn. London/New York, NY: Routledge, pp. 115–152.

Martin, S. (1996) 'Countertrade and Offsets: An Overview of The Theory and Evidence' in Martin, S. (ed.) *The Economics of Offsets – Defence Procurement and Countertrade*. New York, NY: Routledge, pp. 15–48.

Masson, H., Martin, K. (2015) 'The Directive 2009/81/EC on Defence and Security Procurement under Scrutiny', *Recherches & Documents,* no. 03/2015, Fondation pour la Recherche Stratégique, 1 July 2015. [Online]. Available at: https://www.frstrategie.org/web/documents/publications/recherches-et-documents/2015/201503.pdf (Accessed: 14 November 2023).

Maulny, J.-P., Santopinto, F., Schnitzler, G., De France, O. (2023) 'Financing the EDTIB to ensure the security and sustainability of the European industrial model', *Armament Industry European Research Group*, 19 October 2023. [Online]. Available at: https://www.iris-france.org/wp-content/uploads/2023/11/ARES-88-Seminar-Report.pdf (Accessed: 14 December 2023).

Meier, A. (2017) 'European military cooperation: How to defend Europe?', *Euractiv*, 29 November 2017. [Online]. Available at: https://www.euractiv.com/section/politics/news/european-military-cooperation-how-to-defend-europe/ (Accessed: 17 January 2024).

Miszlivetz, Á.J. (2023) 'Compass and Sextant: New Perspectives in the EU's Defence Policy' in Navracsics, T., Schmidt, L., Tárnok, B. (eds.) *On the Way to the Hungarian EU Presidency*. Budapest: Ludovika University Press, pp. 159–168.

Monaghan, S. (2023) 'Solving Europe's Defense Dilemma', *Center for Strategic and International Studies*, 1 March 2023. [Online]. Available at: https://www.csis.org/analysis/solving-europes-defense-dilemma-overcoming-challenges-european-defense-cooperation (Accessed: 5 November 2023).

Mölling, C. (2013) 'Future of the EDTIB at the Defence Council 2013. The German Position, European Realities and December Opportunities' in Masson, H. (ed.) *Defining the European Defence Technological and Industrial Base: Debates & Dilemmas* (I). Fondation pour la Recherche Stratégique, pp. 2–3. [Online]. Available at: https://www.frstrategie.org/sites/default/files/documents/publications/notes/2013/201323.pdf (Accessed: 6 November 2023).

NATO (1949) 'Strategic Concept for the Defense of the North Atlantic Area' *NATO Strategy Documents 1949 – 1969*, 1 December. [Online]. Available at: https://www.nato.int/docu/stratdoc/eng/a491201a.pdf (Accessed: 22 November 2023).

NATO (2023) 'Defence Expenditure of NATO Countries (2014-2023)' *NATO Public Diplomacy Division*, *Press Release*, 7 July 2023. [Online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230707-def-exp-2023-en.pdf (Accessed: 8 November 2023).

Organization for Economic Co-operation and Development (OECD) (2016) 'Defence Procurement' *Brief 23 Public Procurement*, SIGMA Programme, Paris: OECD, Septmeber 2016. [Online]. Available at: https://www.sigmaweb.org/publications/Public-Procurement-Policy-Brief-23-200117.pdf (Accessed: 6 November 2023).

Regulation (EU) 2023/2418 of the European Parliament and of the Council of 18 October 2023 on establishing an instrument for the reinforcement of the European defence industry through common procurement (EDIRPA) (2023) OJ L 2023/02418, 16 October 2023. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2418 (Accessed: 7 December 2023).

Report from the Commission to the European Parliament and the Council on the implementation of Directive 2009/81/EC on public procurement in the fields of defence and security, to comply with Article 73(2) of that Directive (2016) COM(2016) 762 final, Brussels, 30 November 2016. [Online]. Avilable at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0407 (Accessed: 6 November 2023).

Schroeder, G., Sheikh, H., Turkmen, S., Keller, A. (2020) 'Joint ventures to build national defence industries: Beyond offsets', *Strategy&, PwC*. [Online]. Available at: https://www.strategyand.pwc.com/m1/en/reports/2020/joint-ventures-to-build-national-defence-industries/joint-ventures-to-build-national-defence-industry.pdf (Accessed: 17 January 2024).

Schwab, A. (2021) 'Report on the implementation of Directive 2009/81/EC, concerning procurement in the fields of defence and security, and of Directive 2009/43/EC, concerning the transfer of defence-related products', *Committee on the Internal Market and Consumer Protection*, A9-0025/2021, 8 March 2021. [Online]. Available at: https://www.europarl.europa.eu/doceo/document/A-9-2021-0025_EN.html (Accessed: 6 November 2023).

Seguin, B.R. (2007) 'Why did Poland Choose the F-16?', *George C. Marshall European Center for Security Studies*, No. 011, June 2007. [Online]. Available at: https://www.marshallcenter.org/en/publications/occasional-papers/why-did-poland-choose-f-16-0 (Accessed: 11 November 2023).

Siebold, S. (2023) 'NATO urges members to get their logistics homework done', *Reuters*, 23 November 2023. [Online]. Available at: https://www.reuters.com/world/nato-urges-members-get-their-logistics-homework-done-2023-11-23/ (Accessed: 16 November 2023).

Thiel, P., Masters, B. (2014) *Zero to One: Notes on startups, or how to build the future*. New York, NY: Crown Business.

Tigner, B., Landriani, R. (2023) 'Defence acquisition jumps ahead across Europe in 2022, but research lags', *Janes*, 4 December 2023. [Online]. Available at: https://www.janes.com/osint-insights/defence-news/industry/defence-acquisition-jumps-ahead-across-europe-in-2022-but-research-lags (Accessed: 15 November 2023).

Trybus, M. (2014) *Buying Defence and Security in Europe: The EU Defence and Security Procurement Directive in Context*. Cambridge: Cambridge University Press; https://doi.org/10.1017/CBO9780511751462.

Ungaro, A.R. (2013) 'Trends in the Defence Offsets Market', *Istituto Affari Internazionali, Rome, June 14, 2013, Presented at the SIPRI 17th Annual International Conference on Economics and Security (ICES)*, Stockholm, 14-15 June 2013.

US Department of Commerce (2023) 'Offsets in Defense Trade – Twenty-Seventh Study' *Bureau of Industry and Security*. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/sies/3269-public-version-27-annual-offsets-report/file (Accessed: 17 January 2024).

VoxEurop (2023) 'Open letter of academic, military and political figures calling, among others, for a shift to a war economy', 22 December 2023. [Online]. Available at: https://voxeurop.eu/en/biden-help-ukraine-remain-fre-independent-western-countries-must-switch-war-economy/ (Accessed: 25 January 2024).

Witney, N. (2019) 'Building Europeans' Capacity to Defend Themselves', *European Council on Foreign Relations*, ECFR/289, June 2019. [Online]. Available at:https://ecfr.eu/wp-content/uploads/5_Building_Europeans_capacity_to_defend_themselves.pdf (Accessed: 18 January 2024).

World Bank Group (2010) 'Fraud and corruption awareness handbook: how it works and what to look for – a handbook for staff', *Documents & Reports*, Washington, DC, 1 October. [Online]. Available at: http://documents.worldbank.org/curated/en/100851468321288111/Fraud-and-corruption-awareness-handbook-how-it-works-and-what-to-look-for-a-handbook-for-staff (Accessed: 14 January 2024).

The Administrative Arrangement signed between the European Defence Agency and the US Department of Defense (2023). [Online]. Available at: https://eda.europa.eu/docs/default-source/documents/signed-aa-eda-us-dod-2023-04-26.pdf (Accessed: 18 January 2024).

Act in Support of Ammunition Production (ASAP) (no date). [Online]. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/act-support-ammunition-production-asap_en (Accessed: 27 January 2024).

Britain, Japan and Italy sign advanced fighter jet programme treaty (2023) *Reuters*, 14 December 2023. [Online]. Available at: https://www.reuters.com/world/britain-japan-italy-sign-advanced-fighter-jet-programme-treaty-2023-12-14/ (Accessed: 5 January 2024).

A Critical Assessment of the Bundeswehr Procurement Acceleration Act (2022) *Blomstein*, 30 June 2022. [Online]. Available at: https://www.blomstein.com/en/news/a-critical-assessment-of-the-bundeswehr-procurement-acceleration-act (Accessed: 18 January 2024).

Emmanuel Macron warns Europe: NATO is becoming brain-dead (2019) *The Economist*, 7 November 2019. [Online]. Available at: https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead (Accessed: 6 November 2023).

European Defence Industrial Development Programme (EDIDP) (no date). [Online]. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_en (Accessed: 27 January 2024).

European Defence Industry Programme (no date). [Online]. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edip-future-defence_en (Accessed: 2 May 2024).

European Defence Industrial Strategy (no date). [Online]. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en (Accessed: 2 May 2024).

European Defence Investment Programme (EDIP) (no date). [Online]. Available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/european-defence-investment-programme (Accessed: 27 January 2024).

European Peace Facility (EPF) (no date). [Online]. Available at: https://www.consilium.europa.eu/en/policies/european-peace-facility/ (Accessed: 27 January 2024).

Motion for a European Parliament Resolution on the implementation of Directive 2009/81/EC, concerning procurement in the fields of defence and security, and of Directive 2009/43/EC, concerning the transfer of defence-related products, 2019/2204(INI). [Online]. Available at: https://www.europarl.europa.eu/doceo/document/IMCO-PR-658808_EN.pdf (Accessed: 27 November 2023).

The Register of the Certified Defence-related Enterprises. (no date). [Online]. Available at: https://webgate.ec.europa.eu/certider/ (Accessed: 9 January 2024).

A Strategic Compass for Security and Defence (2022). [Online]. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en (Accessed: 27 November 2023).

Standard Eurobarometer 99 – Spring 2023 (2023) *Standard Barometer*, July 2023. [Online]. Available at: https://europa.eu/eurobarometer/surveys/detail/3052 (Accessed: 13 November 2023).

US warns EU over 'poison pill' defence plans (2019) *France24*, 14 May 2019. [Online]. Available at: https://www.france24.com/en/20190514-us-warns-eu-over-poison-pill-defence-plans (Accessed: 17 November 2023).

Versailles Declaration of March 2022 (2022) Versailles, 11 March 2022. [Online]. Available at: https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf (Accessed: 15 November 2023).

Part IV

FIELDS OF INNOVATIONS AND THEIR LEGAL REGIMES

IV.1

DUAL CIVILIAN AND MILITARY USE TECHNOLOGIES: EMERGING AND DISRUPTIVE TECHNOLOGIES

Chapter 6

The Dual Use of Civilian and Military Technologies in the Battlefield of the Future

Jan Mazal

Abstract

This chapter discusses the reasons for and outcomes of the inevitable and dynamic transition to a highly technological future battlefield that will dramatically affect all armies worldwide. Military technology and progress motivation are specific and backed by long-term incremental development, leading to the achievement of pragmatic goals, which are deeply coded in the human genome and are similar for some military and civilian domains, such as battlefields and businesses. This chapter presents fundamental evidence that leads to a better understanding of particular aspects of modern warfare and the technological nature of future conflicts. It discusses the complex relationship between cutting-edge military technology and dual-use aspects and explores the ethical implications and potential future trajectories of such interconnected technological developments.

Keywords: Future Battlefield, Dual-use aspects, Technological Warfare

Jan Mazal (2024) 'The Dual Use of Civilian and Military Technologies in the Battlefield of the Future'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 259–307. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_6

1. Introduction

In an ever-evolving global technological landscape, dual-use innovations weave a complex pattern, serving both civilian and military needs. These tools and systems, which are adaptable to both peaceful applications and strategic military operations, are a testament to human ingenuity.[1] One area where this intersection is particularly profound is in the field of advanced military technologies. While they may originate in defence laboratories with national security and warfare superiority as their objectives, the collateral effects of these military innovations often reshape civilian industries. From the precision of Global Positioning Systems (GPS) to the robustness of aerospace materials, military-derived technologies have, over time, become indistinguishably linked to everyday life. With the advancement of technology, the concept of a battlefield has undergone tremendous change.[2] It now encompasses not only physical locations, but also virtual and digital spaces. Dual-use technologies, with civilian and military implications, have significantly driven this transformation. These technologies shape military strategies, making it crucial to master the digital and technological domains in addition to having physical strength. The conventional interpretation of battlefields as complex terrains dotted with trenches, artillery, and infantry – a depiction deeply ingrained in our minds through history books and war movies – is now undergoing a significant transformation. This traditional image is being reshaped and redefined in the current era of rapid technological advancement.

The term "technological battlefield" refers to the arena in which advanced technologies significantly shape modern warfare, security operations, and defence strategies, powered by artificial intelligence, such as cyber warfare tools, unmanned autonomous systems, space technologies, and advanced communication systems. Significant advantages include enhanced real-time decision-making, remote warfare capabilities, precision targeting, and vast amounts of data that can be collected and analysed. However, with these developments come new vulnerabilities and challenges. Therefore, the technological battlefield demands not only advanced tools, but also new doctrines, strategies, approaches, and a deep understanding of the digital and technological environment that is now interwoven with traditional warfare. Based on current technology and trends in military operations, the following areas of evolution can be considered critical for the technological transformation of the future battlefield:[3]

– Automated and artificial intelligence (AI)-driven warfare: The rise of drones, autonomous vehicles, and AI-driven surveillance systems represents another layer of the technological battlefield. AI algorithms can analyse vast datasets

1 Scharre, 2023, p. 46.
2 Scharre, 2019, pp. 89–112.
3 NATO EDT's, 2024.

for intelligence gathering, and automated drones can execute precision strikes with minimal human intervention.
- Digital frontlines: Cyberspace is emerging as the foremost technological battlefield. Cyber warfare does not involve tanks and troops but is characterised by the presence of hackers, malware, and digital espionage. Nations are investing heavily in the development of sophisticated cyber weapons and defence systems.
- Electromagnetic spectrum and information warfare: Control over the electromagnetic spectrum, encompassing radio waves, microwaves, and visible light, is crucial. Modern information warfare encompasses tactics such as jamming enemy communications, disseminating false information with deep fakes, and influencing public opinion through social media campaigns.
- Dominance in outer space: Once the final frontier of exploration, space is now a strategic battleground. Satellites are essential for communication, navigation, and surveillance and are potential targets. Anti-satellite weapons and satellite defence systems have marked a new age in the space race.
- Biotechnological warfare: Advancements in biotechnology have raised concerns regarding its potential misuse. Engineered pathogens or genetic warfare may become tools in the arsenals of nations or rogue entities, making labs as significant as missile silos.
- Quantum frontiers: As nations race to develop quantum computers, there is a looming battle over quantum encryption and decryption. Mastery of quantum technology may soon become synonymous with global dominance.

In conclusion, the technological battlefield is multifaceted, dynamic, and continually evolving. While traditional warfare objectives, such as dominance, defence, and deterrence, remain unchanged, the tools and terrains have been revolutionised.[4] As technology continues its persistent march, the lines between combat zones and civilian spaces blur, calling for extensive understanding and innovative strategies to navigate this new type of warfare.

Dual-use technology plays a crucial role in the complex relationship between technological progress and strategic military evolution. Its pervasiveness is significant across diverse fields, from the AI domain to material science, and it can fundamentally change conflict dynamics. Dual-use technologies possess high flexibility and blur the lines between peace and war. They have excellent potential to significantly improve operational efficiency, precision, and responsiveness, enabling militaries to collect and analyse vast amounts of data, obtain real-time pictures of joint operations, and develop innovative tactics and strategies. However, the dual-use nature of these technologies raises concerns regarding their proliferation, unintended consequences, and the likelihood of militarising civilian technological advancements. Even though the acceleration of the military technology race offers

4 Scharre, 2023, pp. 11–16.

many complex opportunities and challenges for nations engaged in military affairs, it most likely shape the (inevitable) future world evolvement.

Military history is a narrative of relentless technological innovation. As societies progress, their instruments of war advance in tandem, catalysing profound transformations in battle strategies, tactics, and, ultimately, the outcomes of conflicts. Many military technologies have fundamentally impacted the army and civilian domains, often in ways that blur the lines between these sectors. History demonstrates the far-reaching and frequently unexpected ways in which military innovations can affect civilian life and vice versa. Examples of where dual-use technology has been helpful for both civilian and military purposes could include the following:

Satellite communications Based on satellites positioned in geostationary, medium-, or low-Earth orbits, can transfer data across vast distances. They are situated approximately 35,786 km above the Equator. This technology is crucial for various purposes, including television broadcasting, telephone calls, radio and internet access, military operations, and the emergency sector, connecting disconnected geographical regions. Satellite technology has become a fundamental force in the modern interconnected world.

Long-range earth surveillance enables continuous operational environmental monitoring and is crucial in modern warfare, offering tactical advantages in various combat scenarios. On the civilian front, the same technology has been extensively used in environmental monitoring, disaster management, and urban planning. The utilisation of precision farming methods to enhance crop productivity and resource management holds immense significance in agriculture. The integration of long-range Earth surveillance technology from the military to civilian sectors underscores its adaptability and the possibility of technological breakthroughs that cater to broader societal requirements. This emphasises the interdependence of the military and civilian progress.

Global Positioning System (GPS), initially designed by the U.S. Department of Defense for military navigation, has profoundly transformed civilian life worldwide. In warfare, it provides extreme precision in navigation and targeting, which had not been achieved by any alternative, and significantly supports the military in operation. On the civilian front, GPS has revolutionised numerous industries, from transportation to telecommunications, enabling precise location tracking for navigation, logistics, and personal electronic devices. This technology represents one of the best examples of how military innovation can transcend its initial purpose and become an indispensable tool in everyday civilian life, illustrating the profound impact of dual-use technologies.

The Internet, another crucial example of dual use, was launched as a military initiative called Advanced Research Projects Agency Network (ARPANET) in the late 1960s, initially aimed at maintaining dependable communication during nuclear threats. This early network was essential for enabling long-distance information exchange between computers and served as a vital tool for military purposes. Over

time, this technology has evolved beyond its defence-oriented origin and has become a critical part of the infrastructure for almost every aspect of modern life, demonstrating the transformative potential of dual-use technologies.

Unmanned aerial vehicles (UAVs), commonly known as drones, were initially developed for military purposes and have become essential to modern warfare. This technology outperforms other alternatives in military tasks such as surveillance, reconnaissance, and precision strikes. It has many civilian applications, such as aerial photography, precision agriculture, geographic surveying, and innovative delivery systems.

The development of *nuclear energy* can be traced back to World War II when the United States began the Manhattan Project, which culminated in the creation of atomic weapons. This crucial moment marked the birth of nuclear technology, which was initially intended for the purpose of destruction. Nuclear power plants have emerged as critical players in global energy production because they significantly reduce carbon emissions and reinforce energy security. This transition from wartime innovation to an important aspect of civilian infrastructure represents a significant example of dual-use.

Military medical research advancements in trauma care, prosthetics, and treatment for internal diseases[5] have substantially improved understanding of the requirements of civilian patients, including emergency medical response and rehabilitation.

It is also important to mention the transition of radar and sonar systems from military to civilian uses, such as air traffic control, weather monitoring, and oceanic research. Similarly, advanced materials such as Kevlar and carbon fibres, which were initially utilised in the space and military domains, are now commonly utilised in the private sector (sports equipment, automotive industry, etc.). Jet and rocket propulsion technologies, which are crucial in the military context, have also become integral to civilian air and space industries.

The list of dual-use technologies is long, and a detailed description is beyond the scope of this chapter. However, we should not forget essential areas where dual-use technologies have had a significant impact on both domains, such as robotics, biotechnology, energy storage and battery technology, quantum computing and communications, 3D printing and additive manufacturing, advanced sensors and imaging technologies, telecommunications advancements (e.g. 5G), and augmented and virtual reality (AR/VR). Understanding the dual-use nature of these technologies and their relationship to other non-technological issues is crucial for strategy and policy development.[6]

5 Liu, 2021.
6 Scharre, 2023, pp. 49, 166, 372.

2. Contemporary developments in NATO

The North Atlantic Treaty Organization (NATO) has always been at the forefront of leveraging advanced technology to ensure collective defence, crisis management, and cooperative security. Nevertheless, the reality differs for each Member State. As a result of the collapse of the Warsaw Pact and the corrosion of the Soviet Union's integrity, NATO lost its primary opponent, which has led to a significant erosion of defence capabilities over the last three decades. European armies suffered substantial budgetary constraints, a slowdown in military technological development, and a deterioration in operational readiness.

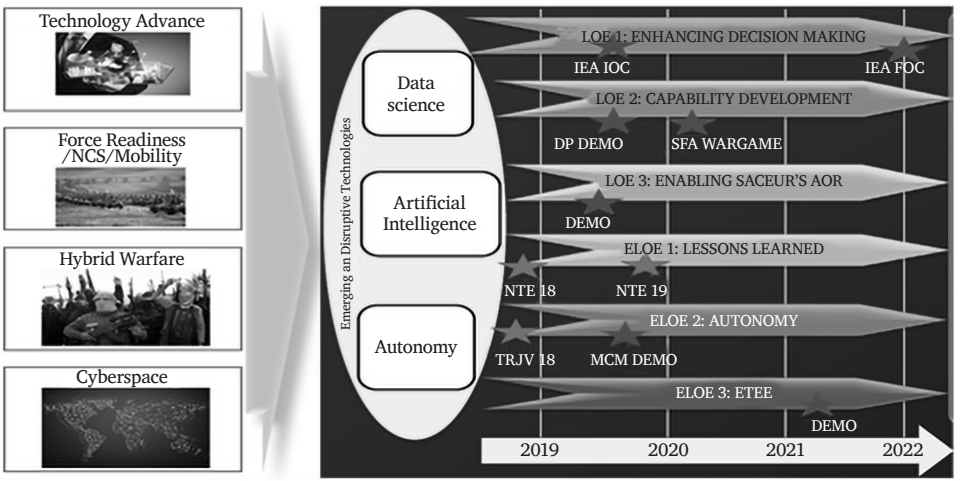
Arguments and prognoses regarding the technological nature of the future battlefield were present within NATO from the 1970s and continued until the beginning of the millennium. Serious discussions about the roles of advanced technologies, especially autonomous systems, started in 2012/2013, focused on the strategic implications of autonomous systems and specific guidelines for managing this field.[7]

In 2016, NATO recognised cyberspace as an operational domain and started reinforcing its cyber defence capabilities. This finding supports the idea that member nations fortify their resilience to counter digital threats. Subsequent progress within NATO, associated with advanced technologies, was introduced at the NATO 2018 Summit as a result of significant technological advancements in China and Russia. The Summit in Brussels was essential for addressing many challenging issues. Key topics included reinforcing defence commitments and increasing Member States' military spending to 2% of their GDP. The summit also dealt with evolving security challenges, such as cyber threats and terrorism, and Russia's growing hostility, especially in the context of its actions in Ukraine. Another significant step was the formal invitation to North Macedonia to begin accession talks, demonstrating NATO's continued expansion and adaptation. The summit highlighted the need for unity and adaptability among Member States to respond effectively to contemporary geopolitical challenges. This led to further discussions on enhancing NATO's readiness and response capabilities[8] in the context of supporting advanced technology development and introducing new and disruptive technologies, crucial for the future NATO evolvement, which led to a significant upgrade of NATO Lines of Effort (LOE).

7 NATO RTO – SAS 097 – *Robots underpinning future NATO Operations* (solved between 2012-2014). [Online]. Available at: https://cmp.felk.cvut.cz/natorobot/index.html (Accessed: 5 January 2024); *Multinational Capability Development Campaign Role of Autonomous Systems in Gaining Operational Access*. [Online]. Available at: https://www.act.nato.int/wp-content/uploads/2023/05/2023_Fact_Sheet_MCDC.pdf (Accessed: 5 January 2024); Kuptel and Williams, 2014, pp. 2–34; Williams and Scharre, 2015, p. 3.

8 NATO, 2018, Article 31.

Figure 1: NATO Summit – Lines of Effort Planned Evolvement, Director of the NATO Modelling and Simulation Centre of Excellence presentation, Steering Committee Meeting 2019



In 2019, space became an official NATO operational domain, highlighting NATO's commitment to addressing the challenges and opportunities presented by satellite communication, navigation, and surveillance. Another significant milestone for the alliance was the NATO Warfighting Capstone Concept (NWCC), which was approved in 2021 and is crucial for reinforcing the alliance's deterrence and defence position. It provides a forward-looking vision for sustaining and enhancing NATO's decisive military edge while adjusting its military capabilities up to 2040. The NWCC primarily addresses the emerging elements of the excessive power race. However, the ongoing conflict in Ukraine initiated by Russia emphasises that the traditional military force remains a crucial aspect of the current security landscape. Since the NWCC's endorsement, NATO has advanced its implementation across various domains, including significant political initiatives, to preserve its strategic superiority.

Last year, the NATO STO released the NATO Science & Technology Trends 2023-2043, comprehensively evaluating emerging and disruptive technologies (EDTs) and their potential impacts on NATO's military operations, defence capabilities, and political decision-making. This emphasises the importance of understanding these trends to guide R&D and innovation activities within the alliance, including capability planning. This report summarises the future landscape of military technologies, considering their increasing intelligence, interconnectedness, decentralisation, and digital nature, which will lead to autonomous, networked, multidomain, and precise military capabilities. It also highlights the dual-use nature of these technologies, which are developed principally in the commercial sector, and the need for NATO to adapt to this dynamic technological evolution to maintain operational

effectiveness. The document lists several EDTs that are expected to impact NATO's strategic and operational capabilities: (i) AI, (ii) Robotics and Autonomous Systems, (iii) Biotechnology and Human Enhancement, (iv) Big Data and Information Communication Technologies, (v) Electronics and Electromagnetics (new supplemental EDT), (vi) Energy and Propulsion, (vii) Hypersonic Technologies, (viii) Novel Materials and Advanced Manufacturing, (ix) Quantum Technologies and (x) Space Technologies.

Although NATO has always considered the critical consequences of technological advancements, its focus on EDTs[9] and other vital areas has increased relatively late. This has led to the need for a dynamic acceleration of advanced technology development and broader stimulation of this sector, which initiated the establishment of the NATO Innovation Fund and the Defense Innovation Accelerator for the North Atlantic (DIANA) in 2021. What led to the intensified effort in collaborative exercise organisations, research activities, and infrastructure investments reflects NATO's cohesive approach to common technology advancement, awareness of the need for responsible development, ethical and interoperability issues, and a unified strategic vision for collective defence and security.

3. Key technology areas and their impact on operational effectiveness and other domains

Based on analyses of the operational needs and recognition of the critical technologies seriously impacting the future operational environment by NATO, EDA, the U.S., and China (supported by Rear Admiral (LH) (Ret.) Cem Okyay[10]), a list of technological areas with serious potential for civilian exploitation (dual-use effect) was identified and further described (most fell under the approved list of "emerging and disruptive technologies" within world-advanced armies).

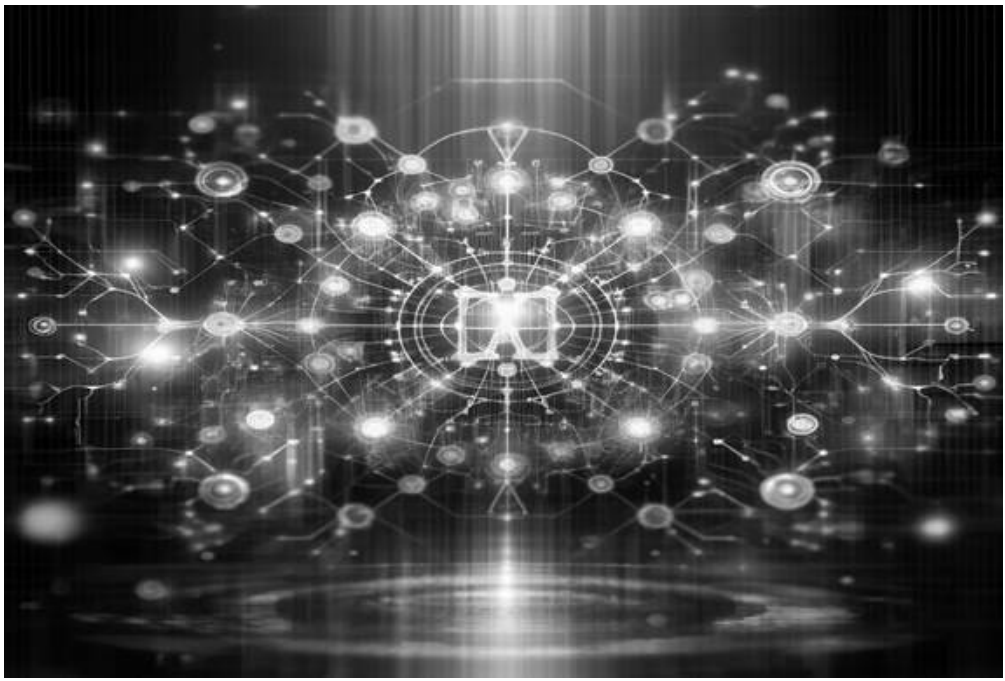
3.1. Artificial intelligence and machine learning

AI and machine learning are not just technological advancements, but have revolutionised paradigms across various domains.[11] These technologies offer transformative capabilities in the domain of operational effectiveness.[12] From predictive maintenance (which forecasts equipment failures before they occur) to advanced data analytics in finance (detecting fraudulent activities in real-time), efficiency

9 NATO EDT's, 2024.
10 Okyay, 2023.
11 Suárez and Baeza, 2023.
12 Johnson, 2023.

enhancement is decisive. Numerous civilian fields have extensively adopted AI. AI-driven diagnostic tools enable early disease detection in the healthcare and logistics fields and machine learning algorithms optimise delivery routes and save time and resources. Moreover, in the defence sector, AI systems enhance surveillance capabilities, process vast streams of intelligent data, and assist or drive autonomous decision-making for drones and other vehicles. These applications have a significant civilian overlap. However, the integration of AI and ML also introduces ethical and security challenges, especially when decisions previously made by humans are delegated to machines. Thus, the pragmatic aspects and influence of AI and ML, while offering unprecedented advantages, call for a balanced approach to harness their potential responsibly and sustainably. AI/ML presents a decisive opportunity for future battlefield dominance,[13] and a nation that has made reasonable progress in this field may quickly acquire the operational and strategic capabilities required to dominate the world. As an example of the visual "creativity" (until recently, an exclusively human domain) of AI, see Figure 2. "How AI sees AI".

Figure 2: How AI sees AI (generated by DALLE.-E in approx. 10 seconds.)



13 Scharre, 2023, pp. 293–299.

3.2. Autonomous systems and robotics

Autonomous systems and robotics represent the convergence of technology and functionality, drastically redefining the operational landscapes across numerous domains.[14] Robots maintain consistently high production standards, unaffected by fatigue or distraction, resulting in heightened efficiency and reduced errors. These systems have also penetrated challenging terrains, from space and the deep sea to autonomous vehicles, promising to transform urban transportation. In the industrial and agricultural sectors, drones autonomously map vast areas and carry various sensors and loads. In the medical domain, robot-assisted surgery outperforms humans in terms of precision and stability. In defence and security, unmanned aerial and ground vehicles are becoming force multipliers, enhancing surveillance and reducing risks to humans. However, as these autonomous systems gain prevalence, they also become a central point of debate regarding job displacement, ethical concerns in decision-making,[15] and potential misuse. The trajectory of autonomous systems and robotics implementation emphasises the importance of adapting and responsibly integrating these tools into society.

3.3. Space technology

Space technology has evolved into a crucial asset underpinning military functions and operational effectiveness. Satellite networks orbiting the Earth have become the focus of modern militaries, providing critical information ranging from precise geolocation data to detailed meteorological insights. These capabilities enhance navigation, surveillance, and communication systems, ensuring that military operations are coordinated accurately and reliably. Space technology also encapsulates the development of missile defence systems, which are essential for national security in developed countries.[16] Furthermore, space assets facilitate a global range of military communications, enabling real-time coordination and strategic decision-making across vast distances. However, this dependency on space technologies necessitates the evolution of new doctrines and defence strategies to protect this strategically crucial extra-terrestrial asset from potential adversaries and emerging threats.

3.4. Quantum technologies

Quantum technologies, rooted in the principles of quantum mechanics, are poised to introduce significant shifts in military operational effectiveness and domains.[17] For instance, quantum encryption promises virtually impenetrable communication

14 Mazal et al., 2019, pp. 53–80.
15 De Mattia, 2022.
16 Manson, 2020.
17 Krelina, 2021.

networks, thereby ensuring the confidentiality and security of critical information. Quantum sensors, which leverage the hypersensitive nature of quantum states, can detect stealth aircraft or submarines with unparalleled precision, negating the traditional concealing advantages. Furthermore, developing a practical quantum computer could revolutionise data processing and analysis, enabling the decryption of previously impervious coded messages and drastically enhancing intelligent operations. Simultaneously, this computational performance can redefine warfare simulations with unprecedented accuracy. However, establishing these quantum capabilities also introduces new challenges. For instance, the race to secure quantum supremacy could destabilise existing power dynamics, and the need to defend against quantum-based threats will demand novel defence strategies. In essence, quantum technologies are not merely tools, but game-changers set to redefine the military strategy and operations landscape.[18]

3.5. Hypersonic weapons

Hypersonic technology marks a transformative development in modern warfare, significantly influencing operational effectiveness in various military domains.[19] Hypersonic aircraft and missiles, exceeding the speed of Mach 5, offer unprecedented operational performance and agility, providing a strategic advantage within immediate response and strike capabilities. High velocity and high-altitude manoeuvrability make hypersonic systems challenging for current missile defence systems.[20] This dramatically shortens decision-making timelines and seriously complicates defensive strategies, potentially necessitating a re-evaluation of existing missile defence doctrines. Furthermore, the dual capability of some hypersonic systems capable of delivering both conventional and nuclear payloads adds a layer of strategic complexity, impacting deterrence dynamics and global security. Advances in hypersonic technology not only enhance operational effectiveness in terms of speed and precision but also significantly influence strategic military planning and international security discourse. The civilian domain (except security aspects) could benefit from this technology in various areas such as space and aerodynamics, for instance, the development of next-generation commercial aircraft that can reach supersonic or hypersonic speeds.

3.6. Internet of Things (IoT)

A vast network of interconnected devices and systems characterises the IoT. It has enormous potential in the military sector for supporting extended operational

18 Scharre, 2023, pp. 37, 39.
19 Cone, 2019.
20 Volkov, 2023.

capabilities and flexibility.[21] Through IoT, assets (ranging from wearable sensors to large-scale military hardware) can seamlessly share real-time data and achieve enhanced situational awareness, thereby improving decision-making accuracy. On the battlefield, IoT-enhanced surveillance systems can detect and transmit threats instantaneously and allow predictive analysis to identify potential critical states or configurations, equipment failures, and vulnerabilities. However, this vast network[22] presents new challenges (such as an increased surface area for potential cyberattacks) that require robust cybersecurity measures to protect the integrity of IoT ecosystems, as such technologies promise a significant shift in military efficiency. IoT in the civilian domain has numerous benefits. One of the main advantages is the considerable enhancement in the efficiency and convenience of everyday life. This improvement is achieved through automation and optimisation of routine tasks, leading to increased productivity, energy savings, and improved quality of life in areas such as smart homes, security and safety, wearable health devices, smart cities, smart grids, climate and environmental monitoring, precision farming, intelligent transportation systems, energy management, and efficiency.

3.7. 5/6G and communication technologies

The emergence of 5G and anticipation of 6G communication technologies have led to significant progress in military operational effectiveness and strategy.[23] These advanced communication infrastructures promise unprecedented data transmission speeds and ultra-reliable low latency, which are critical factors in real-time decision-making and coordination on modern battlefields.[24] For autonomous military assets, such as drones and ground vehicles, these enhanced communication networks enable interoperable communication, fast data sharing, and integration into larger systems. An enhanced bandwidth of 5/6G can support the simultaneous deployment of multiple sensors (from wearable devices for soldiers to advanced radars), allowing for comprehensive situational awareness on battlefields. However, these advances have been challenging. Reliance on high-frequency bands makes the infrastructure more susceptible to interference, requires a denser deployment of relay nodes, and amplifies the risk of cyber threats and electronic warfare tactics disrupting these advanced communication systems. While 5/6G technologies promise to revolutionise military operations and strategic domains, their operational adoption must be accompanied by robust defence mechanisms to protect and optimise their potential, contrary to the civilian domain, where no significant electronic warfare interception is anticipated. The main benefits of 5G and emerging 6G technologies in the civilian domain are that they are compatible with the military; thus, they are a dramatic

21 Manso, 2023.
22 Dahdal et al., 2023.
23 Salor and Baeza, 2023.
24 Ahokangas and Aagaard, 2024.

improvement in connectivity, a critical enabler for remote (real-time) control and complex interactions, supporting economic growth and innovation, public safety, remote work, and education.

3.8. Cloud computing

With its centralised data storage and processing capabilities, cloud computing has become increasingly essential for modern military operations.[25] This technology enables the efficient aggregation, analysis, and dissemination of vast datasets, enabling militaries to achieve enhanced situational awareness and faster decision-making, instead of relying on different and localised databases. Forces across land, air, sea, and cyber domains can access and contribute to a unified information pool, high-performance computing hardware (HW), and centralised software (SW) services, ensuring compatibility across various devices, coordination, and synergy within military operations. For instance, training simulations, computer-assisted exercises[26] (CAX), military logistics, and staff administrative tasks can be easily optimised and coordinated, offering scalable solutions adaptable to a particular operational demand. However, data centralisation poses security concerns because potential cyberattacks on these cloud infrastructures can compromise vast collections of sensitive information. The primary advantage of cloud computing for civilian and military applications is its notable improvement in the accessibility and scalability of computer resources and services. This technology allows individuals and organisations to access vast computing resources, data storage, and various applications and services over the Internet without substantial investment in physical hardware. The main benefits include accessibility, flexibility, on-demand resources, cost-effectiveness, rapid deployment, quick updates or innovation, enhanced data management, easy collaboration, reliable infrastructure, security enhancements, overall energy efficiency, and sustainability.

3.9. Biotechnology and human augmentation

Biotechnology and human augmentation converge to redraw the boundaries of what is possible in the military, pushing human capabilities and resilience to another level.[27] Advances in biotechnology offer solutions, such as rapid wound healing, enhanced resistance to physical and psychological stress, and the potential to operate in extreme environments with minimal protective equipment. Human augmentation, from exoskeletons and augmented senses (beyond standard human

25 Blakley et al., 2022.

26 Computer assisted exercises use a real time computer simulated operational environment for improving staff readiness in operations, and military decision making. They are recognized for their cost efficiency and effectiveness in reducing risk while facilitating multinational participation from different locations.

27 Hutcheon, 2021.

capabilities) to neural interfaces, enhances the operational efficiency of soldiers and extends mission endurance. These advances also introduce ethical dilemmas, potential vulnerabilities, and questions regarding the long-term impact of augmented personnel. Moreover, closer biotech integration increases the risk of cyberphysical attacks, potentially becoming a new dimension of warfare. Although biotechnology and human augmentation have immense potential to redefine military effectiveness, they have serious ethical, strategic, and security implications that must be resolved in advance. These fields are at the forefront of medical developments in the civilian domain. Thus, these technologies have the potential to dramatically improve the quality of life, extend lifetime, and increase human performance, impacting the fields of medical breakthroughs and therapeutics, disease treatment and prevention, regenerative medicine, prosthetics and implants, sensory and cognitive enhancement, genomic medicine, diagnostic tools, and ageing research.

3.10. Cybersecurity and cyber resilience

In an age when the cyber domain is as critical as the physical domain, cybersecurity and cyber resilience have emerged as essential components of military operational effectiveness.[28] As modern armies integrate sophisticated technologies, from drones and AI-driven intelligence systems to advanced communication networks, their dependency on cyber infrastructure has increased exponentially. Despite offering unprecedented operational benefits, the cyber domain is a domain for cyber warfare and is susceptible to hostile operations by adversaries, namely, cyberattacks.[29] Cybersecurity is both a technical requirement and a strategic imperative. Beyond defence, cyber resilience (the ability to anticipate, withstand, recover from, and adapt to adverse cyber events) is crucial, as it ensures that military operations can continue despite cyber adversities and adapt rapidly to evolving threats. Integrating cybersecurity and cyber resilience enhances military capabilities, shifts doctrines from old-fashioned offences, and defends against robust digital protection and adaptive recovery. This new paradigm upgrades modern military operations, encompassing battles in physical and virtual (cyber) domains. The military domain, like others, has a significant interconnection with its civilian counterpart, and in some cases, these domains share particular hardware and software resources and physical infrastructure. The primary aim of cybersecurity and resilience in the civilian domain is the comprehensive protection of the digital ecosystem, ensuring the security of personal information, continuity of critical services, and the overall trust and reliability of the digital infrastructure. These technologies and principles are crucial to the functioning of the modern world and are thus extremely important.

28 Hallaq, 2017.
29 Salomon, 2022.

3.11. Big data analytics

In today's digital era, militaries are overwhelmed by the vast amounts of data linked to the Common Operations Picture (COP) update and processing. Big data analytics emerged as a critical tool[30] for transforming data flows into actionable intelligence and strategic insights. The employment of advanced algorithms and computational hardware enables patterns to be uncovered, highlighting anomalies, anticipating adversarial steps, optimising resource allocation, ensuring the timely and efficient deployment of assets, and making informed and prompt decisions.[31] Beyond operational efficiency, big data analytics provide a strategic vantage point, enabling militaries to understand geopolitical trends, predict potential conflict zones, and adapt strategies accordingly. However, data-driven decision-making introduces serious challenges, such as dependency on accurate and valid data, complex validation, and algorithmic-based vulnerabilities (necessitating particular oversight). The Big Data approach is expanding, even in the civilian domain, providing deep insights into complex datasets for optimal decisions, and improving personalisation, operational efficiency, public services, healthcare, financial stability, environmental sustainability, and education. Experience from practice and reciprocal evolution would be beneficial to both domains.

3.12. Advanced materials and manufacturing

Progress in advanced materials and manufacturing involves the transformation of military capabilities in various areas, primarily combat resistance, logistics, and sustainment.[32] Dynamic evolution in material science (such as super-lightweight composites and unique metamaterials absorbing or shaping electromagnetic waves) has enabled the development of advanced military equipment or assets. Similarly, advanced manufacturing techniques, such as additive manufacturing or 3D printing, offer flexible and rapid production of complex components.[33] This allows parts to be manufactured in remote locations, even on battlefields. This capability accelerates repair and maintenance and reduces the logistical burden of transporting unnecessary spare parts.[34] Additionally, integrating intelligent materials with unique attributes such as self-repair, self-shaping, and environmental adaptation promises to extend the lifetime, adaptability, and maturity of military assets. These advancements have dramatically enhanced military operational effectiveness and introduced new challenges and responsibilities. This field significantly overlaps with the civilian domain, in which the main benefits of advanced materials and manufacturing are

30 Govindaraju, Raghavan and Rao, 2015, pp. 260–262.
31 Ravi, 2021.
32 NATO EDT's, 2024.
33 Mamalis, 2019.
34 Hahn, 2019.

apparent, grounded in enhancing product performance and sustainability. Examples of advanced materials include carbon-fibre composites, graphene, shape-memory alloys, self-healing metals, polymers and elastomers, fullerenes, carbon nanotubes, nanocrystals, biodegradable polymers, and superconductors. However, as these advanced materials and manufacturing techniques become more prevalent, they also require new training, maintenance, and manipulation standards and considerations regarding recyclability, environmental impact, and other issues.

3.13. Energy and propulsion

Developing advanced energy and propulsion technologies is crucial for enhancing the operational effectiveness in all military domains. Advancements in this field, include, for instance, new generations of engines, energy storage (batteries), alternative fuels, and innovative propulsion methods,[35] which could dramatically expand the performance of all military assets with prolonged endurance, safety, higher speed, and payload, thus enhancing operational superiority and strategic reach. The potential of dual-use energy and propulsion technologies in the civilian domain is apparent; however, these areas do not always converge because their principal objectives differ (operational effectiveness vs. environmental and economic factors). The main benefits include a significant increase in energy efficiency, cost reduction, and a potential transition towards cleaner and sustainable energy sources, which supports the urgent need to reduce greenhouse gas emissions and slow global climate change. Examples of energy and propulsion technology with dual-use potential include nuclear fusion, propulsion and microreactors, electric and hybrid-electric propulsion systems, directed energy transmission technology (lasers[36] and high power microwaves), hypersonic propulsion, power based on changes in buoyancy, solar photovoltaics and concentrated solar power, advancements in battery technology[37] such as solid-state batteries, development of ultra-fast charging and wireless charging technology, hydrogen fuel cells, energy smart grids and microgrids, advanced biofuels, and space-based solar power.

3.14. Directed energy weapons

Directed Energy Weapons (DEWs), which include systems based on laser and high power microwave technology, are likely to significantly improve operational effectiveness.[38] This is supported by critical advantages that allow them to outperform contemporary systems or approaches. These benefits arise from extreme precision and speed-of-light engagement, which provide revolutionary tactical advantages in

35 Guillaume et al., 2019.
36 Rezunkov, 2021.
37 Wasim et al., 2022.
38 U.S. DOD, 2023.

all scenarios and activities. Tactical experience shows that the capabilities of DEWs can be effectively applied to high-speed and small targets such as incoming artillery shells, small drones, and rocket barrages, which present a game changer in tactics and situations that obsolete technology cannot manage.[39] Moreover, DEWs have a low cost per shot compared with conventional munitions, offering economic efficiency in prolonged engagements. Their almost unlimited magazine capacity ensures sustained operation in extended conflicts, as long as power is available.

The operational effectiveness of DEWs is also apparent in their stealth characteristics. These weapons produce minimal exposing effects (sound and visible signatures), rendering them hard to detect and trace back. Furthermore, the adaptability of DEWs to various platforms, from handheld devices to naval ships and aircraft, demonstrates their versatility in various military fields. While DEWs are primarily associated with military applications, the primary technologies and principles of directed energy have significant potential benefits in various civilian sectors, such as material processing, additive manufacturing, optical communications, power transmission, wildlife protection, vegetation control, laser surgery and therapy, non-lethal crowd control, search and rescue operations, remote sensing, material science, and indirect material diagnostics.

3.15. Adaptive education and training

Adaptive education and training technology[40] are critical components for future military training and improving human operational effectiveness. This technology employs an advanced conceptual framework of high-fidelity simulations, virtual reality VR- and AI-driven learning platforms to create personalised and immersive training programmes for individuals to achieve optimal learning.

By leveraging these technologies, military training has become more intensive, engaging, and realistic, focusing on the areas of knowledge and skills that require improvement. Adaptive training technologies also allow new information and tactics updates to be quickly disseminated across the armed forces, ensuring that military personnel stay up-to-date with the latest trends and operational developments. Moreover, these technologies contribute to cost-effectiveness by reducing the physical infrastructure or resources needed and enabling the simultaneous training of large numbers of personnel. The benefits of adaptive education and training in the civilian domain highly overlap with those in the military, and technological advancement in both domains can contribute to improvements in the civilian education.

39 Del Monte, 2021.
40 Durlach, 2012.

3.16. Blockchain technology

Blockchain technology, often associated with cryptocurrencies, has found innovative potential within the military, promising enhanced security, transparency, and administrative simplicity.[41] A blockchain is a decentralised register that ensures data integrity through cryptography, making unauthorised alterations extremely difficult. In the military, blockchain can authenticate supply chains, providing information on the origin and quality of equipment. The communication system offers a tamper-proof record for intelligence operations, ensuring the authenticity and integrity of critical information exchanged. Moreover, blockchain can ensure transparency and traceability in complex defence contracts and procurement networks, thereby reducing bureaucratic issues and potential corruption. This technology also has possible implications for secure voting systems for deployed troops and transparent personnel authentication. However, as with any technological integration, there are some challenges to consider. The scalability and energy consumption of blockchain solutions, especially in large-scale applications, require optimisation, and although blockchain holds significant promise for modernising various military domains, its integration requires careful consideration and adaptation. In the civilian domain, blockchain technology already supports cryptocurrencies such as Bitcoin, Ethereum, Ripple, and Litecoin, but its applications extend far beyond digital currencies.[42] It has been adopted in various sectors, including finance, supply chain management, healthcare, and identity verification, owing to its potential to provide secure and transparent solutions to many complex problems involving trust and transaction verification.

3.17. Electronics and electromagnetics

Integrating advanced electronic systems and electromagnetic technologies into the military could dramatically increase situational awareness, real-time decision-making, precision targeting, secure communication, stealth capability, manoeuvrability, and other areas, thereby amplifying the efficiency and strategic capabilities of the armed forces. The miniaturisation and performance increase of electronics and electronic warfare[43] capabilities towards smaller, lighter, multipurpose, flexible, and energy-efficient devices has enabled the deployment of advanced and game-changing systems, such as micro-drones, nano-robots, micro-radars, EW interceptors, jammers, spectral analysers, wearable bio-integrated electronics, human-augmented devices, next-generation surveillance equipment.. Such technology is characterised by quality and performance, which could drastically outperform an obsolete asset

41 Bikos and Kumar, 2022.
42 Krichen et al., 2022.
43 *Electromagnetic warfare*, 2023. [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_80906.htm (Accessed: 12 January 2024).

and tactical approaches on the future battlefield, applied in an offensive or defensive/protective manner. For example, the latest research demonstrates the revolutionary potential of plasma shields to high power microwaves, seriously impacting anti-drone warfare.[44] The dual-use nature of these technologies is significant and omnipresent within our everyday lives, extending the civilian domain of advanced electronics and communications we rely on. Any advancement in this field will immediately affect both domains.

3.18. Brief summary

The current era of military development is characterised by a mosaic of technological advancements in many areas. These changes are not just minor improvements but are transformative forces that redefine operational effectiveness and strategy. They provide military precision, speed, and adaptability, enabling more nuanced and informed real-time decision-making. However, these advances have resulted in new vulnerabilities and ethical considerations. As the boundaries between the digital, physical, and biological domains become increasingly unclear, a comprehensive defence approach that integrates advanced tools, robust countermeasures, continuous training, and ethical frameworks is required. The future of military operations, shaped by this technological renaissance, offers unimaginable opportunities and significant challenges requiring a balance between innovation, responsibility, and anticipation.

These areas exhibit substantial overlap and dynamic evolution. Any additional motivated acceleration could lead to the achievement of specific milestones and revolutionary progress in these areas sooner or later, benefiting society. Although opinions differ, an escalation of the armament race and development does not generally align with the philosophical values of modern society. However, the contemporary world is not uniform in this regard, as the history of humankind shows that conflict has been deeply rooted in human nature and shaped by our survival instincts since ancient times. This will significantly affect current and future security environments, and effective strategies to address these issues are needed.

---

4. Main aspects of military advanced technology within future warfare

The future battlefield is anticipated to differ vastly from traditional combat zones shaped by rapid technological advancements and changing geopolitical dynamics. Based on contemporary trends and estimations, integration of a vast number of

44 Impact Lab, 2024.

advanced technology components is expected, with a critical dependency on the cyber domain and a severe impact on other areas, such as information warfare and psychological operations. These factors will lead to a dynamic and complex environment in which the future landscape of threats is also expected to transform considerably with the rise of non-state entities and the prevalence of asymmetric warfare. The probability of global conflict has risen with the evolution of the world security environment. This shift demands that military strategies should be flexible, integrate diverse advanced technologies, enhance cyber capabilities, and employ innovative and unconventional approaches to counter the complex challenges of these conflicts.

4.1. Performance-oriented battlefield – the result of a fundamentally pragmatic approach

The logical assumption, derived from industrial domains and trends, is that future battlefield evolution will be driven by a highly pragmatic approach, leading to cost/benefit optimisation, which will inevitably discriminate against some redundant military approaches and dogmas. The critical reasons for contemporary changes or transition to a highly technological battlefield are the level of maturity of operationally proven or effective advanced military technology and its expected dynamic evolvement (proven by experience and supporting trust in the future technology operational performance). This has led to a reconsideration of contemporary approaches and focused attention on future military development strategies. One of the critical aspects of this activity is the evaluation of the perspectives of human (as a centric entity around military operations or activities) performance versus advanced technology in the short- and mid-term vision. This is coupled with complex considerations regarding the cost-effectiveness and physical limitations of technological and biological systems.[45] The main limitation is human reaction time and the speed of action, which are critical not only for close combat activities but will be decisive for operational reasoning in the future.

From an operational perspective, it seems that the centre of gravity is an open and independent focus on the critical objectives of the military effort, which have not changed significantly over the centuries, such as threat elimination, occupying territory, conquering areas, and defending a sector. If we abandon the need to maintain certain (usually old-fashioned) dogmas in orientation towards achieving these goals, which typically complicate[46] the effective approach to the solution, we open up space for mathematical modelling of these activities and subsequently

45 While the "production and training" of human soldiers could take several decades, the manufacturing of technical systems could take minutes or seconds.

46 These complications could arise from dogmas like: 'the commanders experience and intuition are the backbone of his decision-making process, 'only the human decision will be accepted for execution', 'combat formations will follow only the approved doctrinal rules', 'territory could be considered as a conquered only when the foot of the friendly soldier touch it'.

advance automation and optimisation of operational multi-criteria processes leading to the selected goals. This is a crucial conceptual and philosophical transition process for military systems based on pure pragmatism, leading to a future performance orientation that seems dynamic and unpredictable, especially from a mid-to-long-term perspective. This is because there is a lack of adequate options for regulating this process in the contemporary world. Even so, we might pinpoint crucial components or areas that have pivotal or central functions and experience notable changes such as automation of combat and decision-making activities, logistics and supply chain efficiency, adaptive training and education strategies, cost-effective solutions and flexible, "on-demand" serial production automation, resilience and rapid development of countermeasures, international collaboration and partnerships, and biotechnology and bio-augmentation.

As most of these areas have a serious overlap with the civilian domain, there is a strong assumption that (in our globalised world) progress in the military domain will quickly affect another domain and vice versa. The direction of innovation flow usually reflects the amount of investment and the attention paid to a particular area. Based on the global deterrence and increases in defence budgets, there is a logical expectation of a dynamic military innovation pace we have never experienced before, backed by advanced technologies and an extraordinary military performance orientation we remember from the Cold War. From a logical and pragmatic point of view, we could expect a broader and more intensive hybridisation of future warfare and an extension of the battlefield to more expansive areas of states and neighbouring countries. From a philosophical perspective, there are parallels between the military and civilian domains grounded in the principles of Industry 4/5.0, driven by the particular performance aspects pursued.

4.2. Transition to an AI Command-and-Control in future military operations

Based on previous and contemporary operational experiences and the evolution of modern warfare, there is a solid and logical assumption that the future battlefield will require a new concept of the command-and-control[47] (C2) approach at all levels of command.[48] The initial idea of this transition was introduced in the Defense Advanced Research Projects Agency (DARPA) "Deep Green"[49] project in 2008. This comes with a fundamental shift in the so-called OODA (observe, orient, decide, act) loop[50] paradigm in the context of the expected increase in battlefield dynamics

47 Command and Control (C2) in a military context refers to the exercise of authority and direction by a designated commander over assigned and attached forces in the accomplishment of a mission. It is a fundamental concept in military operations, playing a crucial role in organizing, directing, and coordinating military activities.

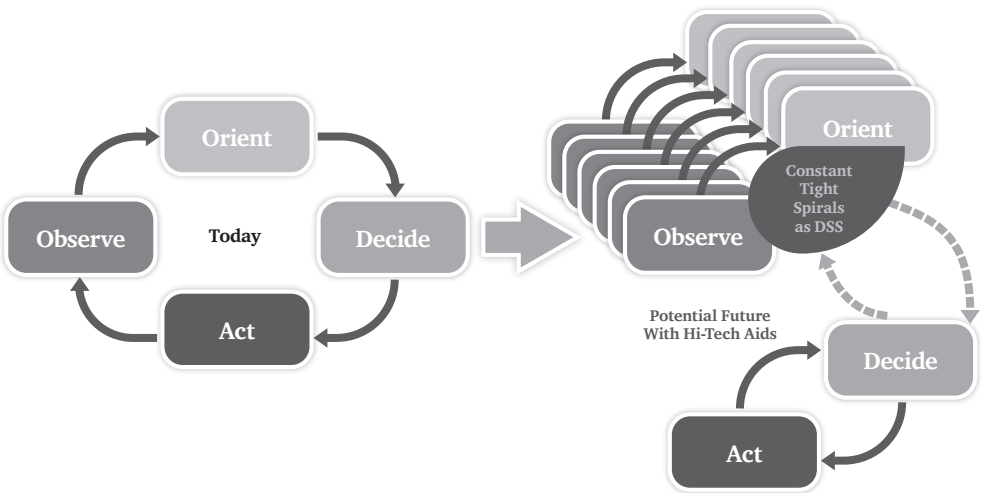
48 Sarcia and Colo, 2023.

49 Surdu and Kittka, 2008, pp. 4–12.

50 Originally formulated by military strategist John Boyd, the OODA loop was initially a sequential process. Each phase followed the other linearly: observe, orient, decide, and act.

(arising from a logical assumption of the reduction in reaction/response times and the enormous growth of tactical entities on the battlefield). In this highly complex operational environment, obsolete C2 (management) principles and approaches are no longer effective.[51] While the systematic, original OODA serial approach often resulted in delayed responses, it was a disadvantage in high-tempo combat environments, where the expected operational dynamics increased up to a level that caused the old-fashioned reactive approaches to no longer be effective. Due to the reactions practically settling in place, the situation usually varies significantly from when the particular Course of Action (COA[52]) is planned. The original "Deep Green" OODA upgrade forecast, becoming an indisputable fact today and remaining critical for the future, requires serious changes in the military concept of decision-making processes, and the traditional serial OODA loop must be parallelised.

Figure 3: Graph of the serial OODA paradigm transition to the parallelised version



The parallel OODA loop paradigm revolutionises the deeply rooted military decision approach and incorporates simultaneous actions across different phases. This approach significantly accelerates decision-making and injects a level of dynamism and flexibility previously unreachable in the serial model. It also promotes a more decentralised command hierarchy, empowering lower levels of command

51 Black, 2024.

52 Course of Action (COA) refers to a plan or method proposed and developed to achieve a specific mission or task. It outlines how available resources (such as troops, weapons, equipment, and time) can be used to deal with a specific situation or to accomplish a particular objective. The development and analysis of COAs are integral parts of the military planning process.

with autonomy to react swiftly, informed by real-time data, and a comprehensive understanding of the broader battlefield context and higher echelon commanders' intentions. Incorporating advanced technologies, such as high-fidelity wargaming[53] constructive simulations,[54] AI,[55] and integrated communication networks, further amplifies the capabilities of the parallel OODA loop. These OODA upgrades facilitate rapid information processing and sharing, enabling cohesive and synchronised actions among military forces, which are pivotal for ensuring quick, strategically coherent, and contextually relevant combat responses. This fact, backed by the evolution of modern computing technology, will inevitably result in a transition to an AI-enhanced C2 system in future military operations. The key factors for a successful transition of current C2 to AI-aided/driven C2 and its potential dual-use aspects are understanding the fundamental role of C2 in the military, the role of automation in C2 systems (C5ISTAR),[56] increased confidence in using cutting-edge technologies, improving situational awareness, autonomy, and warfare automation (within C2), and international cooperation.

4.2.1. The role of C2 in the military

C2 creates a fundamental framework within military operation management and is integral to orchestrating the use of military forces during warfare. The C2 philosophy enables military commanders to plan, direct, and control forces to accomplish assigned tasks. C2, supported by the military decision-making process (MDMP),[57] involves gathering and processing information, making decisions, executing them, and monitoring outcomes, emphasising flexibility and responsiveness during military engagements. A practical C2 framework emphasises the establishment of a transparent command hierarchy, resilience of communication networks, and optimisation of decision-making processes. Real-time information exchange is pivotal for commanders to evaluate the operational state of a battlefield accurately, seek and coordinate effective COAs, and disseminate commands. Thus, the efficiency of the

53 Wargaming in the military context is a decision-making tool that simulates conflict scenarios or battles to test strategies, develop and evaluate courses of action, and predict their outcomes without actual combat. This practice allows military leaders and planners to anticipate potential challenges and outcomes in a controlled, risk-free environment.

54 Constructive simulation in the military context is used primarily for training, analysis, and decision support. It involves the creation of a virtual environment where hypothetical scenarios are played out, often for the purposes of training, strategy development, or decision-making analysis.

55 Tarraf, 2022.

56 C5ISTAR is an acronym representing a broad set of functions and capabilities in modern military operations. It stands for Command, Control, Communications, Computers, Cyber (C5), Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR). This framework encompasses a number of activities and technologies fundamental to military operations.

57 The military decision-making process (MDMP) is a detailed, step-by-step process used by military commanders and their staff to develop and plan military operations. It provides a structured framework for analysing a situation, developing options, and deciding on the best course of action.

C2 framework is critical for maintaining the tempo of operations and ensuring that military responses are coherent and aligned in real-time with opponents' reactions. With technological advances, C2 evolved to incorporate network-centric operations that leverage information superiority and collaborative engagement to achieve strategic advantages. Modern C2 systems aim to seamlessly integrate intelligence, surveillance, reconnaissance, and operational planning to empower decision-makers at all levels, creating the so-called C5ISTAR systems (pushing C2 theory to an advanced technological framework).

Although C2 is connected to the military, philosophically, C2 and the civilian domain closely overlap within the management field. Thus, any theoretical upgrades to the C2 conceptual framework could be reflected in the dual-use aspects that are already present, mainly in security areas (level of command, hierarchy, responsibility delegation, etc.).

4.2.2. C5ISTAR systems

The military term C5ISTAR covers various technologically advanced components and processes that are essential to modern warfare and military operations. This concept represents the high-level integration of systems and activities that the armed forces utilise to secure and maintain information superiority in operations through real-time analysis of the COP[58] The historical roots of these systems can be traced back to the development of telegraphy and radio in the 19th century. These technologies have enabled militaries to communicate over long distances, leading to critical breakthroughs in the art of warfare. These systems have continued to develop with an extremely high degree of technical integration and complexity. These systems collect and process information from numerous sources, including remote sensors, satellites, automated drones, robots, and social media. There are many emerging trends in C5ISTAR technology in the prognosis and estimations of the future battlefield, which raises many concerns and requirements, such as real-time advanced processing of an enormous amount of battlefield data generated every second (the amount of data is expected to increase exponentially in the future with an increased number of next-generation sensors and system deployments). This has led to several outcomes, the major one being the application of AI (with a focus on ML) to automate tasks and improve decision-making. Another trend is the development of cloud-based C5ISTAR systems, which can provide global access to information and resources. As mentioned, C5ISTAR systems are essential to modern warfare because they provide militaries with the information and tools they need to succeed on the battlefield. Nonetheless, a conceptual similarity exists between several civilian management systems across numerous fields, from industry to security and government.

58 A common operations picture (COP) is a single, identical display of relevant operational information that is shared by more than one command. It is a critical tool for situational awareness and decision-making in military operations.

4.2.3. Building trust in advanced technology

Trust in military technology is essential for the success of defence operations and is achieved through rigorous operational testing and validation (OT&V). OT&V is the empirical backbone that ensures that new technologies perform as required under the broadest spectrum of battlefield conditions. The process of OT&V encompasses a systematic evaluation from the early developmental stages to field trials and post-deployment assessments, encapsulating the effectiveness and survivability of technological solutions in operational settings.

To the greatest extent possible, OT&V processes must be transparent and comprehensive, including scenarios that reflect current and anticipated mission challenges (cyber threats, electronic warfare, extreme physical environments, and countermeasures). The results of these tests are fed back into the development loop to improve the design, tactics, training, and maintenance protocols. OT&V also facilitates user familiarisation, an often-overlooked factor that is critical to the successful adoption of new military technologies. Moreover, trust is established by demonstrating the technology's adherence to ethical standards and rules of engagement, ensuring that it aligns with legal and moral constraints under the laws of war. This aspect of trust is fundamental, as technological advancements, such as AI and autonomous systems, present new ethical dimensions for warfare.

OT&V is an indispensable part of the defence technology lifecycle. It underwrites the functionality and safety of new systems and cultivates the trust and confidence of war fighters who rely on these systems, thereby ensuring that the human element remains at the heart of technological advancement in military operations. The military sector is usually highly conservative, and building trust in new and revolutionary technologies takes time. Any mistake or technology failure can result in serious latency extensions or technology rejection. This area resembles many civilian fields where trust depends on positive experiences linked with reliability and performance, which are critical, such as autonomous transportation, the aircraft industry, the IT sector, and cybersecurity. Specific improvements in this area could potentially be used in the civilian domain.

4.2.4. Improved situational awareness

Improved situational awareness is crucial for operational efficiency and domination within the information domain. As decision-making processes become more complex and are supported by a fusion of real-time intelligence, long-range surveillance, and data-driven insights, potential options become vast, requiring additional processing and an enhanced understanding of battlefield relationships. This element becomes much more significant when we add a temporal dimension to the battlefield's state space, which is required to identify potential future crucial configurations.

This highly complex and multidimensional mathematical model of the battlefield must be processed in real-time using cutting-edge computational algorithms and

supercomputers to extract extensive datasets to identify patterns and trends, exposing the concealed operations of adversaries and signalling emerging threats. The prompt analysis of such data allows military commanders to make rational decisions with unprecedented accuracy and preventive judgements. Although much work has been done on AI implementation within tactical scenario analyses and planning,[59] the complexity of the contemporary battlefield introduces many challenges and reveals gaps, which are areas of current and future research linked to quantum computers and advanced AI technology, and have become one of the central fields of technological competition in the military.[60] All modern armies are searching for comprehensive situational awareness technology that enables a more agile and precise allocation of resources, timely responses to emerging threats, and more coordinated manoeuvres, ultimately leading to superior tactical and strategic outcomes.

4.2.5. The role of autonomy and warfare automation in C2

Autonomy and automation will inevitably play transformative roles in future military operations, reshaping strategies and tactics across various domains and must be integrated within the C2 area. Integrating autonomous systems will enable militaries to execute complex missions with greater efficiency and reduced risk to human personnel. However, this opens up an additional dimension of challenges and problems the military has never previously faced. The main problem lies in effectively managing a potentially extreme number of these entities in the future, especially within a communication-restricted environment. This challenge leads to the pursuit of hybrid or distributed architectures and complete autonomy in particular areas of defence technologies.

As these technologies advance, they will augment existing capabilities and create new operational paradigms where human-machine relations become essential for achieving strategic objectives. However, this shift requires careful consideration of the ethical, legal, and operational implications, ensuring that the integration of autonomy and automation aligns with established military values and objectives. Nevertheless, the comprehensive automation of military components, assets, and the C2

59 NATO STO SAS-139. [Online]. Available at: https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-SAS-139/$$TR-SAS-139-ALL.pdf (Accessed: 15 January 2024); SAS-150, SAS-166, MSG-189, AVT-382. [Online]. Available at: https://www.sto.nato.int/publications/Pages/default.aspx (Accessed: 15 January 2024); MCDC – FUT-LEAD. [Online]. Available at: https://www.act.nato.int/wp-content/uploads/2023/05/2020_mcdc-futlead.pdf (Accessed: 15 January 2024); HPE/HPO. [Online]. Available at: https://gids-hamburg.de/wp-content/uploads/2021/04/2021-03-22_MCDC_HPEO_Project_Report_final-1.pdf (Accessed: 15 January 2024); MUAAR. [Online]. Available at: https://www.act.nato.int/wp-content/uploads/2023/05/2020_mcdc-muaar.pdf (Accessed: 15 January 2024); InfoAgeC2. [Online]. Available at: https://cdissz.wp.mil.pl/u/MCDC_Overview.pdf (Accessed: 15 January 2024).

60 NATO STO SAS-164, 21st Century Force Development, (2020-2022). [Online]. Available at: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-OCS-ORA-2023/MP-SAS-OCS-ORA-2023-05.pdf (Accessed: 15 January 2024).

framework seems inevitable for the armed forces to perform effectively on the future battlefield.

4.2.6. International cooperation

International cooperation and standardisation in the military C2 domain are essential for creating a cohesive and efficient framework for joint multinational operations. In coalitions of weaker nations, there is typically no other way to counter a powerful adversary effectively. The standardisation process includes harmonising communication protocols, data formats, operational procedures, and technological systems as well as joint training and exercises to evaluate the fundamental principles of that effort. Organisations such as NATO have professionalised such efforts, developing standardised practices and technologies that member countries adhere to and facilitating interoperability and cooperation. Nevertheless, achieving even essential standardisation is a complex and long-term process involving negotiations and compromises among participating nations, each with unique military practices and strategic priorities. Despite these challenges, the pursuit of standardisation in international military cooperation remains a critical goal, as it significantly strengthens the collective ability of allied nations to respond to global security challenges in a coordinated and effective manner.

4.2.7. Brief summary

The integration of AI into C2 structures and systems is primarily motivated by the need to rapidly process and understand the vast amounts of data generated from various components, systems, sources, and sensors (satellites, sensors, ISR, military entities, cybersecurity systems, etc.). As warfare becomes more network-centric and data-driven, traditional human-centric C2 systems will struggle to keep pace with the speed and precision required for operational decision-making, and this is happening in the contemporary world. AI can offer quick predictive analytics, automated planning, and real-time threat assessment, thus enhancing situational awareness and operational planning, which play a decisive role on the battlefield. The shift towards AI-enhanced C2 is expected to unfold progressively as AI technology matures and proves its reliability and effectiveness in military applications. This transition will likely be gradual, beginning with AI as a decision-support tool and evolving into more autonomous functions such as trust in technology development. The timeframe for this evolution depends on technological advancements, operational testing, the validation of AI systems, and the establishment of ethical and legal frameworks for their use in military settings. By the late 2020s or the early 2030s, we might see a more noticeable integration of AI into C2 systems, marking a significant shift in how military operations are conducted.

4.3. Swarming, Autonomy, and Real-Time issues as fundamental future military attributes

As predicted in the 1980s and demonstrated in the latest conflicts, autonomous systems are revolutionising warfare in the 21st century, marking a paradigm shift in the military domain. These systems, which range from drones and unmanned vehicles to AI-driven sensor networks, have dramatically changed the nature and dynamics of modern combat operations. The critical aspect of autonomy in modern warfare is its potential to conduct operations faster, for longer durations, and with a level of precision that is challenging for human-operated systems.

Beyond individual tasks, autonomous systems contribute to a broader network-centric warfare approach, operating in extreme numbers as a fully integrated multi-robot system, and communicating and coordinating actions simultaneously to achieve operational goals quickly and effectively. Based on the principles of algorithmic behaviour, the large swarms of autonomous systems present a critical threat, and the effectiveness of coordinated swarms could be exponentially increased (compared with uncoordinated swarms). Such swarms could outperform any contemporary defence system by quickly flooding the engagement area with an enormous number of robotic entities ready to be sacrificed in favour of mission objective fulfilment.

Another factor that favours autonomous systems is their low latencies and unprecedented reaction speeds. The future effectiveness of warfare depends heavily on the ability to respond within the shortest possible time. Human reaction times typically vary between 200 and 250 milliseconds, and reaction times tend to slow down with ageing.[61] In contrast, electronic systems can theoretically respond in less than a millisecond, in practical scenarios, between 30 and 50 milliseconds. This shift towards autonomous warfare enhances military capabilities and reshapes engagement, decision-making, and force-deployment principles. Systems with autonomous features continue to undertake roles exclusive to humans in previous decades, and this trend seems to be evolving exponentially. However, as these systems become more prevalent, they also raise important ethical, legal, and strategic questions, particularly regarding decision-making in combat situations and the future role of human soldiers. Autonomous systems have significant military potential in various fields, which could also be utilised in civilian domains and could bring substantial benefits, such as:

- Enhanced situational awareness – due to the advanced sensing and information processing,
- Reduced risk to humans – due to the distant or automatic control,
- Increased operational efficiency – due to advanced automation, unprecedented performance in time-critical operations, and enormous numbers of coordinated systems applied

61 Woods et al., 2015, p. 10.

– Precision and accuracy – enabled by advanced mechatronics and electronics advancements.

Various autonomous systems play essential roles in the modern military landscape, each contributing unique capabilities to defence strategies. Typically, these systems are arranged according to their operational domains, covering the most common applications.

– Unmanned aerial vehicles (UAVs) and drones are becoming increasingly prominent and are being utilised for reconnaissance, surveillance, and precision strikes.
– Ground-based autonomous vehicles such as unmanned ground vehicles (UGVs) and unattended ground sensors (UGS[62]) enhance logistics, surveillance, and battlefield support capabilities.
– Autonomous naval systems are transforming maritime operations into unmanned surface vehicles and underwater vehicles (UUVs). They play critical roles in mine detection, anti-submarine warfare, and oceanographic research by providing greater operational reach and requiring less human interaction.

There is expected to be an extension to the space domain and potentially new domains in future warfare (for instance, underground, human mind[63]). All the mentioned systems overlap significantly with civilian domains (such as transportation, surveillance, supervision, and security), and any technological breakthrough in these areas will inevitably lead to an increase in trust within the civilian domain and encouragement for a broader spectrum of its applications. Because military requirements are usually much higher than those in civilian domains (even in industrial or security areas), limitations in the legal framework and cost-benefit analyses are the primary obstacles to civilian adoption of military technology, in addition to technology maturity issues.

4.3.1. Key Challenges and Limitations of Autonomous Systems

Although they offer significant advantages and capabilities, autonomous systems face many critical challenges that affect their development, deployment, and effective operation, such as technical complexity, AI and ML limitations, coordination, communication, safety, reliability, human–machine interface, integration of cyber vulnerabilities, and regulatory and standards development. Although the detailed list and description of these challenges significantly exceed the framework of this chapter, two significant challenges of contemporary autonomous systems limit their comprehensive employment in operational applications. Although numerous promising solutions and theoretical approaches exist, it will likely take several years of

62 UGS could also refer to the term unmanned ground system, which some armies use instead of UGV.
63 Gregg, 2016.

additional development to reach an operational readiness state. These challenges are navigation in complex environments (in all domains) and automated operational reasoning and coordination.

4.3.2. Autonomous navigation

One of the most challenging tasks for unmanned systems, especially in the ground domain, is "off-road" autonomous navigation,[64] which proves the DARPA RACER[65] challenge released in 2021. Despite being theoretically solved[66] no solution has yet been effectively implemented, which introduces a key milestone for the explosion of UGV applications across all areas in the future. The critical part of "off-road" navigation is the correct "cost-map" calculation within the path planning process, which is theoretically solved. Nevertheless, it places a high demand on several sensors (such as the Light Detection and Ranging (LIDAR), camera, RADAR, and Hyperspectral sensing), data processing, and traversability calculations to implement Multi-Body Simulations (MBS) physical vehicle simulations and integrate other machine learning principles and methods. This theoretically proven approach is hard to apply in real-time with contemporary in-vehicle computing technology, and currently, it is one of the most important research topics within the autonomy domain.

UAV navigation is a very complex problem as well, but due to the 3D path planning options (in contrast to the ground, which is only 2D) and usually an "obstacle-friendly environment", it is far easier to compute and optimize in real-time. It has been proven over two decades of extensive experience in military applications and civilian expansion. One of the most challenging issues within the UAV domain today is the coordination of many entities in an obstacle-dense environment, which concentrates a significant research effort on this field. Nevertheless, advanced concepts and demonstrators[67] that perform an effective UAV swarm motion through dense woods and jungles already exist. Thus, potential military applications are in sight, with the potential to dramatically change combat tactics and efficiency.

4.3.3. Operational reasoning

Tactical autonomy is one of the complex and critical capabilities of future autonomous systems that will enable them to effectively replace soldiers on the battlefield.[68] AOR is based on COP quantification (math transformation), modelling, and automated friendly force COA delivery in the context of the latest battlefield configuration and extreme levels of detail for global plan consolidation for each automated

64 Loganathan and Ahmad, 2023.
65 Ackerman, 2022.
66 Thakker, 2021.
67 Gent, 2020.
68 Hagos and Rawat, 2022.

tactical entity. Several approaches exist to find a solution to this problem, and one of the initial concepts was introduced in the DARPA Deep Green project; however, complexity, computation and communication issues, lack of deep understanding, and operationally successful experiments prevent this field from evolving dynamically, even though it is extremally important for dominance on the future battlefield. More comprehensive information on individual approaches and solutions can be found online.[69]

These technological challenges have significant dual-use effects in various civilian fields and, like in the military, will be critical milestones in the automation of a series of tasks that severely impact particular human domains, such as transportation, forestry, the mining industry, critical infrastructure supervision and service, and project management.

5. Military technology impacts human domains and dual-use aspects

Integrating advanced technology into the military significantly affects various human domains within this unique environment, such as the social, psychological, cognitive, and cultural aspects. Sophisticated communication tools and networks have altered the dynamics of interactions among military personnel, enhancing coordination and potentially creating dependencies on digital forms of communication. The demands of operating advanced technologies can increase competency requirements and stress, particularly in high-stakes or combat situations. Advanced technologies require the development of new skills, continuous learning, and adaptation. While advanced technologies bring numerous operational advantages to the military, their influence on individuals requires careful organisation to reach their full potential while protecting military personnel's mental resilience, health, and readiness. The following specific domains show how sophisticated military technology has affected the human domain (which could benefit from the technology itself or experience from military operational domains):

5.1. Social Impact

Sophisticated communication networks and collaboration platforms have revolutionised how military personnel communicate and coordinate, overcoming geographical barriers and enabling the real-time and efficient exchange of information. However, this reliance on digital communication can also affect traditional face-to-face interactions, potentially affecting unit cohesion and developing interpersonal

69 Mazal, 2022; Mazal, 2020.

relationships that are crucial for teamwork in high-pressure environments. Technology has reshaped military social relations by introducing diverse and remotely operated platforms, leading to shifts in traditional roles and responsibilities. This evolution requires adaptations in the command structure and operational culture, posing challenges and opportunities for social integration and establishing effective team dynamics. Additionally, because of advanced technology, digital connectivity brings the external world closer to military personnel, even in deployed locations, thereby impacting the traditional boundaries between service members' professional and personal lives. While advanced technology offers significant operational benefits, its influence on the social aspects of military life requires careful consideration to maintain robust, cohesive, and adaptable military communities. This aspect is also valid in the civilian domain, and research on sociotechnological impacts could benefit from military experience in advance.

5.2. Psychological impact

The psychological impact of advanced military technologies is fundamental and complex, influencing the mental health and operational mindset of military personnel.[70] On the one hand, these technologies can improve soldiers' capabilities, situational awareness, and safety, which can boost their morale and confidence. Tools such as exoskeletons, enhanced surveillance systems, and AI-assisted decision-making platforms can reduce the physical stress and fatigue of warfare and improve the psychological status of personnel. On the other hand, the high risk factors of operating sophisticated technology in life-or-death situations can elevate stress levels, leading to increased pressure and anxiety. The remote nature of advanced warfare technologies such as drones can also create psychological distance from the battlefield, leading to unique challenges in processing combat experiences and outcomes. Moreover, the rapid pace of technological change requires continuous adaptation and learning, which can be mentally demanding. Concerns about overreliance on technology and the potential loss of fundamental military skills may also contribute to psychological tensions. Thus, while advanced technologies in the military have significant tactical advantages, their psychological impacts are complex and require a comprehensive approach to ensure military personnel's mental resilience and readiness, taking into account that reliance on advanced technologies with a lack of understanding of its functionalities and impacts is inevitable and introduces a significant challenge for the future of man-machine relations (this aspect has many counterparts in civilian jobs, from the air traffic controller to the police officer).

70 Lovalekar et al., 2018.

5.3. Cognitive impact

The effect of advanced military technologies on cognition is a critical aspect of modern warfare that significantly influences how military personnel perceive and process information,[71] make decisions, and adapt to complex environments. These technologies often enable enhanced data processing and provide situational awareness tools, aiding quicker and more informed decision-making under pressure. Advanced AI technology can augment cognitive abilities by filtering and prioritising vast amounts of information, allowing soldiers to focus on high-level strategic thinking rather than being overwhelmed by data. However, this reliance on technological assistance also raises concerns about cognitive atrophy – potentially diminishing essential skills such as navigation, observation, and instinctual decision-making–traditionally improved through experience and practice. Moreover, constant interaction with advanced systems requires a high level of cognitive flexibility and continuous learning, as soldiers must keep pace with rapidly evolving technologies and shifting operational paradigms. This need for constant upskilling can be mentally stimulating and demanding, highlighting the need for balanced cognitive engagement and training with careful consideration of the cognitive load and training methodologies. In the future, the trend of advanced automation, sensing, and AI processing within almost all domains will inevitably lead to a dramatic reduction of mental load in humans, enabling individuals to focus on strategic goal selection and supervision over mid to long-term periods. The acceleration of this trend in the military domain will immediately affect the commercial (mainly but not only industrial) sector and vice versa.

5.4. Economic impact

The economic impact of advanced military technologies is complex and influences national budgets, the defence industry, and broader economic landscapes. Investments in advanced military technologies can impose a significant financial burden on governments. However, the beneficial outputs associated with research, development, and acquisition can potentially lead to improvements in different sectors, as human history has proven. The defence industry significantly contributes to technological innovation, creating employment opportunities and promoting economic growth. This often sets the pace for commercial technological development and leads to strategic opportunities, in that countries at the forefront of military technology may acquire geopolitical advantages that could affect the dynamics of economic power and global commerce. Thus, although advanced military technologies demand considerable financial and human resources, they also act as catalysts for technological progress and economic development, underscoring the need for strategic and balanced investments.

71 Billing, 2021.

5.5. Cultural impact

The cultural impact of advanced military technologies extends beyond the boundaries of defence and influences broader societal perspectives, values, and narratives. These technologies often become symbols of national pride and power, shaping a nation's cultural identity and global perceptions. For instance, aerospace, nuclear, AI, missile, and other military technological advancements reflect a country's scientific and technological achievements, inspiring national cohesion and ambition. However, there has also been a cultural shift in the perception of warfare and the military's role, driven by technologies that change the nature of combat. This shift can lead to debates and re-evaluations of challenging traditional martial values and hero archetypes. Moreover, the integration of advanced technologies into military training and operations affects the culture within the military itself, altering traditions, practices, and soldiers' experiences. Thus, while these technologies are primarily tools of defence and security, their cultural consequences are significant and shape narratives, values, and perceptions within and beyond the military sphere.

5.6. Environmental impact

The environmental impacts of advanced military technologies are a growing concern, with both direct and indirect effects on global ecosystem. Developing, testing, and deploying these technologies can have significant ecological consequences, considering that advanced military technologies are associated with accelerating the arms race, increasing weaponry production, and worsening environmental impacts in multiple sectors. While the primary focus of military technology is national security, there is increasing awareness and responsibility towards minimising its ecological footprint. This involves implementing more sustainable practices in production, operation, and disposal and considering the environmental impacts of designing and developing new technologies. Balancing these considerations is crucial to ensure that efforts to enhance defence capabilities do not come at the cost of environmental health and sustainability, as in other domains (forestry, energy production, intensive agriculture, space, transport, and many others).

5.7. Political impact

The political impact of advanced military technologies is essential and far-reaching, as it influences the dynamics of international relations and domestic policy decisions. Countries with cutting-edge military technologies often possess significant geopolitical influence on the global stage, using their technological superiority for diplomacy or deterrence. Developing and deploying these technologies can shift the balance of power, leading to strategic alliances, softening tensions, and increasing the pace of the arms race. Domestically, the decision to invest in advanced military technologies can be a sensitive political issue that is often debated in

terms of national security priorities versus other societal needs. These technologies also shape defence policies and military doctrines, influencing how nations perceive and respond to threats. Furthermore, the use and export of military technology can become a significant consideration in foreign policy, affecting international trade agreements and diplomatic relations. The governance and regulation of these technologies impose substantial political challenges, requiring cross-border cooperation and the establishment of international rules and agreements. Thus, advancing military technologies is not just a matter of defence; it is also linked to national policy, affecting the domestic and international geopolitical landscape.

5.8. Ethical aspects and strategic implications

The ethical and moral implications of advanced military technologies are increasingly coming to the forefront of the defence discourse, posing philosophical questions and challenges.[72] Technologies such as autonomous weapons systems, AI-driven decision-making tools, and enhanced surveillance capabilities have raised significant ethical dilemmas with potentially critical strategic consequences. For example, delegating essential combat decisions to automated systems raises issues of accountability, responsibility, and the moral implication of reduced human oversight in life-and-death situations. The potential for AI to make decisions based on algorithms that may not fully understand complex human ethical considerations adds another layer of concern. Within this area, a series of terms and standards describe the level of autonomy, automation,[73] or level of human involvement within automated processes, such as (i) Human-in-the-loop – a concept where a human operator is directly involved in the decision-making or control process of a robotic system, (ii) Human-on-the-loop–a concept where a human supervisor monitors and oversees an autonomous system but does not directly control each of its actions, and (iii) Human-out-of-the-loop – a concept where humans are not actively involved in controlling, monitoring, or intervening in the operations of the robotic systems.

The use of advanced surveillance technologies and cyber warfare tools also raises privacy issues, and there is potential for abuse of power, affecting both combatant and civilian populations. These technologies also force a re-evaluation of the established norms and laws of warfare, challenging traditional conceptions of

72 Committee on Ethical and Societal Implications of Advances in Militarily Significant Technologies that are Rapidly Changing and Increasingly Globally Accessible, 2014.

73 Autonomy levels, particularly in the context of autonomous vehicles, are typically defined on a scale that measures the degree to which a system is capable of operating without human intervention. Multiple versions of these scales exist, but they all essentially describe the spectrum between the manned and fully automated (autonomous) systems. The Society of Automotive Engineers (SAE) defines these levels for vehicles as follows: Level 0 – No automation, Level 1 – Driver assistance, Level 2 – Partial automation, Level 3 – Conditional automation, Level 4 – High automation, Level 5 – Full automation.

honour, courage, rules of engagement, and combat ethics. Integrating advanced technologies into military operations requires a broader ethical agreement and algorithmic (logical) framework (what-if), clear guidelines, and ongoing dialogue among military leaders, policymakers, ethicists, and the wider society to navigate these complex moral affairs responsibly. In the international environment, various campaigns and initiatives have aimed to establish ethical frameworks for employing advanced military technology. These campaigns often involve international organisations, governments, nongovernmental organisations (NGOs), academic institutions, and sometimes the military and defence industries. The key focus areas are as follows:

- Autonomous weapons systems: Initiatives such as the Campaign to Stop Killer Robots focus on a pre-emptive ban on developing and using lethal autonomous weapons systems (LAWS).
- Cyber Warfare: With the increasing prevalence of cyber warfare, attempts are being made to create global standards and ethical principles for cyber operations (especially those targeting civilian infrastructure and noncombatants).
- Artificial Intelligence in Warfare: Organisations such as the Institute for Ethics and Emerging Technologies and the Future of Life Institute focus on the ethical use of AI in military contexts, promoting regulations that prevent misuse and ensuring that AI is developed and used in alignment with human values.
- Nuclear Non-Proliferation and Disarmament: Groups such as the International Campaign to Abolish Nuclear Weapons (ICAN) work towards the global elimination of atomic weapons, emphasising the catastrophic humanitarian consequences of their use.
- Biotechnology and Chemical Weapons: Campaigns like the International Committee of the Red Cross focus on the ethical implications of biotechnological advances in warfare, encouraging commitment and strengthening of international laws like the Chemical Weapons Convention and Biological Weapons Convention.
- Surveillance and Privacy: With advanced technologies enabling unprecedented levels of surveillance, campaigns have focused on balancing national security interests with individual privacy rights, such as those led by the Electronic Frontier Foundation.
- Military AI Research Oversight: Academic and research groups have called for responsible AI research in military applications, emphasising the need for ethical oversight and transparency in military-funded AI research projects.
- International Laws and Treaties: Efforts are being made to update and expand the existing international humanitarian laws and treaties to incorporate new technologies and ensure that they are used in compliance with international law and ethical standards.

Ethical campaigns and initiatives play a crucial role in shaping the discourse around developing and deploying advanced military technologies, aiming to influence policymakers and the public towards an international consensus for responsible and ethical technological advancement in defence. While these activities are crucial for guiding accountable development and use, they present serious risks and challenges, such as:

- Innovation slowdown: Strict ethical rules or calls for technology bans may obstruct innovation and research, putting a nation or alliance at a strategic disadvantage, particularly if potential adversaries continue to develop such technology. Furthermore, they may have negative economic impacts on the defence industry, which is a significant part of many countries' economies.
- Difficulties in reaching consensus: The existence of diverse ethical, cultural, and political viewpoints worldwide leads to challenges in reaching a consensus on regulations. International policies may contain conflicts or inconsistencies owing to ethical divergence between nations.
- Rapid pace of technological advancement: The rapid pace of technological advancement can surpass the development of ethical frameworks and regulations, resulting in a gap where new technologies are used without comprehensive ethical guidelines.
- Dual-use dilemmas: Strict regulations based on ethical campaigns may unintentionally delay beneficial civilian technological advancements and applications of many advanced military technologies with dual-use applications.
- Enforcement challenges: Enforcing ethical guidelines globally is challenging due to varying capabilities and priorities in different countries. Noncompliance or private development of banned technologies can pose significant issues.
- Security dilemmas: The development of military technologies often leads to security dilemmas in which nations feel threatened and respond with their developments, escalating an arms race.
- Public perception and trust: These campaigns may cause people to fear or mistrust advanced technologies, leading to resistance to their beneficial use.

While ethical debates are essential for building consensus on the responsible use of advanced military technologies, there is a significant risk of overestimating particular issues, based on artificial or unrealistic scenarios. These scenarios, while well-intentioned, could be subtly influenced by potential opponents to achieve specific goals. Thus, any activity within this scope should maintain a deep and rational understanding of all the discussed areas and possible aspects guided by competent personnel.

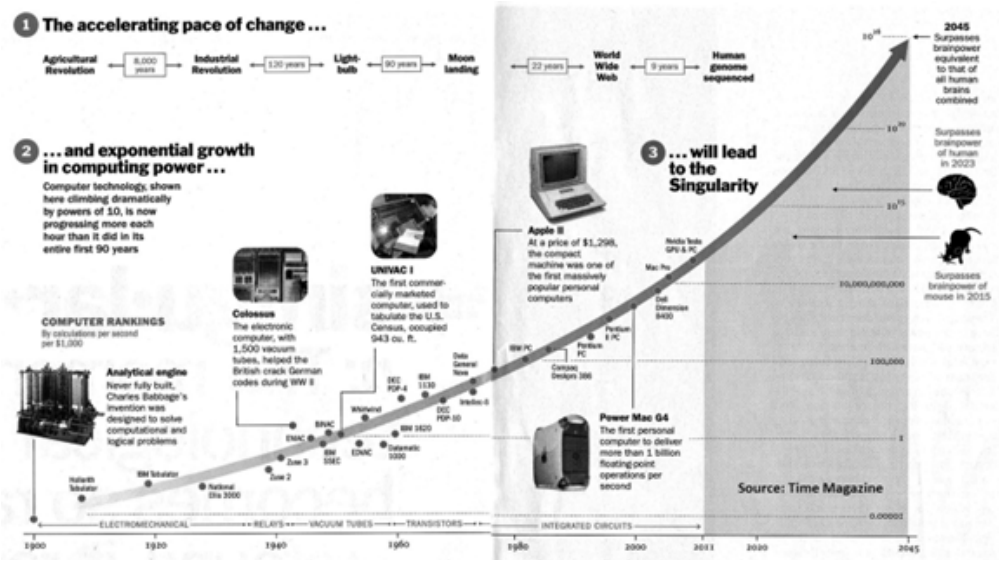
5.9. Short and mid-term future uncertainty

An accurate prognosis is crucial for achieving future goals and operational efficiency within the security environment. Unfortunately, it is fundamentally impossible to predict the future of complex socioeconomic systems accurately. Concerning the chance of a correct prognosis based on contemporary facts and development trends, there is only a slight chance of estimating short or mid-term future evolution in the military. However, we can track some historically proven and correct estimations in the military, such as:

- Guerrilla warfare: Mao Zedong and Che Guevara predicted that guerrilla warfare would be effective against conventional military forces. This warfare became effective in the 20th/21st centuries, and their prediction has been proven in many conflicts, such as the Vietnam War, the Cuban Revolution, and various African and Asian independence movements.
- Blitzkrieg: Heinz Guderian, inspired by the ideas of British military strategist J.F.C. Fuller and others, forecasted the effectiveness of fast and intensively coordinated combat using tanks, aircraft, and motorised infantry. This proved highly effective in the early years of World War II.
- Nuclear warfare: Albert Einstein and Winston Churchill forecasted the devastating potential of atomic weapons, which led to a doctrine of mutually assured destruction during the Cold War. This doctrine was maintained throughout the Cold War to prevent large-scale conflicts.
- Air superiority: Theorists such as Italian General Giulio Douhet argued in the 1920s that air power would decide future wars. This has been proven in many conflicts, and air superiority is critical in almost all wars.
- Cyber warfare: In the late 20th and early 21st centuries, experts began predicting the rise of cyber warfare, such as hacking, and digital disruption in military strategies. One example is the Stuxnet virus attacks on Iranian nuclear facilities, and there are many other instances of cyberespionage and sabotage.
- The rise of drones: Military analysts have predicted that drones will be extensively utilised in warfare. This prediction has become true in modern conflicts in which drones have replaced human soldiers in their battle roles and have significantly altered the nature of warfare.

However, the rapid pace of technological advancement and its impact on global society make predictions even more difficult in today's operating environment. This creates considerable uncertainty and has drawn the attention of many technological experts and futurologists. Kurzweil's path to singularity shows how computing power (a single supercomputer) is growing exponentially, surpassing the performance of the human brain in 2021 and potentially of all humanity by 2045 (see Figure 3).

Figure 4: Ray Kurzweil's prediction on the path to singularity (source: Time Magazine)



However important, computing performance is required to surpass the human intellect, and the critical aspects of intelligent machines lie in the complexity of AI algorithms, which can compete with humans at all levels of intelligence. We distinguish between two levels of AI intelligence: weak and strong.

Weak intelligence, also known as narrow AI, refers to a type of AI that is designed and trained for a specific task. Unlike strong AI, which aims to replicate human-like awareness and cognitive abilities, weak AI operates within a limited predefined range or context and is programmed to perform specific functions. It does not possess the understanding, consciousness, or ability to apply knowledge or skills to contexts beyond its specific software design. Examples of weak AI are present in everyday life and include virtual assistants, recommendation systems, facial recognition, and email filtering. The development of weak AI has significantly contributed to efficiency in various sectors by automating routine tasks, enhancing user experience, and improving decision-making processes through data analysis. Weak AI already competes with or significantly outperforms the human brain in various tasks[74] such as imagery recognition, planning, and desk game performance, and this trend continues within the broader AI field.

74 *A graph showing how artificial intelligence (AI) has overtaken humans and overtaking them is like this*, 2017.

Figure 5: AI visualisation of the path to singularity (source: DALLE-E)

Strong AI (Artificial general intelligence) refers to a type of AI that can understand, learn, and apply its intelligence to solve any problem with the same level of development as a human brain. The characteristics of Strong AI are as follows:

- Generalised learning ability
- Understanding and reasoning
- Consciousness and self-awareness

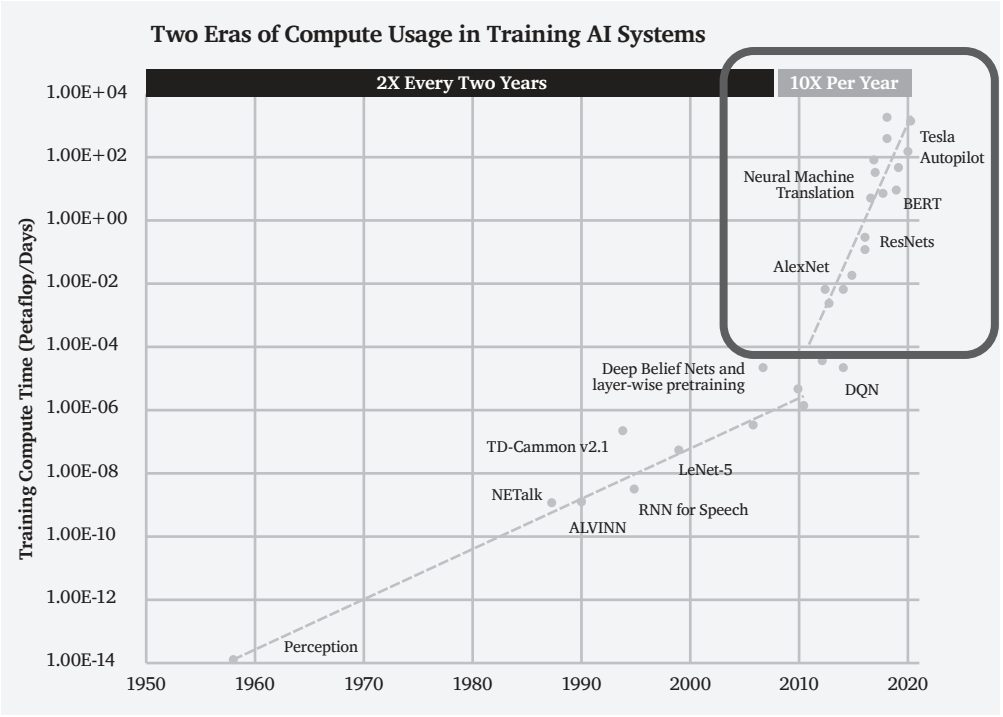
Strong AI remains a theoretical concept, and there is no clear evidence that an initial successful solution is yet in sight. In any case, it provides an extremely attractive and mind-breaking social theme with significant ethical, philosophical, and technical challenges, including the nature of consciousness, the rights of artificial entities, and their impact on society.

Nevertheless, based on the development trend of AI performance, mainly coming from the deep neuronal network field, there is a dramatic increase in performance that overcomes Moore's law (Moore's law is the theory that the number of transistors on an integrated circuit will double approximately every 1.5 years. According to James Wang,[75] a former NVIDIA (a US AI leading company) engineer who was part of launching the GeForce Experience, the advancement of AI is 5 to 100 times faster

75 *Artificial intelligence is growing dozens of times faster than Moore's Law*, 2020.

than Moore's Law, as illustrated in Figure 6. As the necessary conditions for General AI gradually reach readiness, its emergence in the near future seems increasingly realistic. However, the impact of General AI on the future remains highly uncertain and could easily be seen as a subject more fitting for science fiction.

Figure 6: Graph of AI performance growth compared to Moore's law (source: ARK Investment Management LLC, "AI and Compute", OpenAI)



5.10. Recommendations for policymakers, military strategists, and tech developers

The effective development of military technology has seriously affected national security and strategies. In light of potential opponents' technological advancements, the government should be vigilant in preventing any potential loss of operational performance that cannot be compensated for through other strategies like diplomacy, human force superiority, or environments that prohibit the use of certain technologies. The effective development of any technological sector relies on several simple (though practically challenging) principles that must be considered and carefully maintained, such as:

– Continuous evolvement – Any development area suffers from breaks and restarts, leading to the loss of skilled and experienced personnel.. Adequate

technological progress necessitates continuous evolution and incremental capacity increases based on needs and conditions.
- Budget: An appropriate budget is foundational for the effective development of military technologies, enabling sustained innovation, attracting and retaining talent, maintaining advanced research facilities, and responding to emerging threats. It is crucial to accomplish the entire technology development lifecycle from initial R&D to full-scale deployment.
- Infrastructure This includes local facilities and a broader interconnection within the scientific and industrial community to create an efficient architecture of departments and institutions that provide and maintain excellence in particular technological areas.
- Human capital encompasses the knowledge, skills, and abilities that individuals possess and which are essential for every stage of the technological development cycle, from research and development to production and deployment.
- International cooperation plays a fundamental role in advanced development and offers several key advantages. Challenges usually do not outweigh the positives of state-of-the-art awareness, resource sharing, specialisation and expertise, standardisation and interoperability, innovation, cross-pollination of ideas, access to markets and technologies, and enhanced cooperation in other areas.

6. Conclusion

The experience gained from the history of warfare is that the level of technological progress is a crucial aspect that cannot be compensated for in any other way (like numerical superiority). This fact directly touches on issues such as the fundamental nature of warfare and operational effectiveness; these issues inevitably lead to the development of autonomous machines with capabilities (and cost) against which humans will no longer be able to perform effectively because of their very rapid response capabilities. Currently, we are still at the beginning of our understanding of this phenomenon. However, current technological demonstrators and simulations clearly show the development lines of the future battlefield, where it will no longer make sense to deploy human soldiers because the fight between human soldiers and autonomous robots will inevitably lead to the loss of human lives). Therefore, the robotisation of combat will be crucial for dominance on the modern battlefield, and the technological superiority of autonomous systems will play a decisive role.

From a global perspective, the world is in a relatively advanced stage of robotisation and implementation of AI, and many initial demonstrators have shown the

immense short- and medium-term potential of robotics. Many new components are already available, and must be integrated or modified for specific purposes.

One of the most critical components of autonomous systems is coordinated swarm behaviour (focusing on a common operational goal), particularly in the context of enormous numbers of these entities on the battlefield, which will become a dramatically different environment from the relatively slowly evolving battlefields today. Without a doubt, technology will shape the nature of close-quarters combat in the future. The current conflict in Ukraine, where tens of thousands of drones are employed daily, is a clear example of the logically pragmatic repercussions of this reality.

Based on the prognosis from various sources, state-of-the-art technology, and the evolution of contemporary combat (Ukraine, Gaza. etc.), several critical technologies and areas are expected to shape the future of military development and warfare, closely linked with potential dual-use effects in this decade.

Advanced simulation technology will be a key component of future military dominance on the battlefield. The use of mathematical modelling and simulation[76] is a key trend[77] in scientific, industrial, and other domains for more than three decades. The quality of the solutions obtained through modelling and simulation depends on the nature of the problem being solved and the environment in which the simulation occurs. Simulation fidelity is on the rise to deliver unprecedented detail within augmented environment complexity, enabling advanced analysis and decision-making, implementation of AI and machine learning models, virtual reality (VR) and augmented reality (AR) systems, combat simulation software and streaming platforms, interactive digital maps and geographic information systems (GIS), Cyber Warfare, Logistics Support, and Unmanned Systems Simulation. The development of advanced military simulation technologies could inspire and motivate civilian applications with a particular military overlap from government strategy to industry and security, with the pursuit of maximum performance and cost-effectiveness.

AI and machine learning will play an increasingly important role in various fields, such as data analysis, predictive analytics, autonomous systems, and decision-making processes. Nowadays, LLMs[78] have been sufficiently developed to reduce the workload of staff members responsible for routine administration. As is known from the past, they will bridge the gap between now and fully automated combat

76 This discipline aims to "virtualize" problems by converting them into a virtual domain on computers that approximates the real world, through mathematical models and computer simulations.

77 The primary reason for this approach is that a many problems have become so complex that it is impossible to find a direct solution through analysis. As a result, the so-called evolutionary method is often used, where input parameters are experimentally adjusted to meet the desired output of the simulation.

78 LLM stands for "large language model". This refers to a type of artificial intelligence model that is specifically designed to understand, generate, and interact with human language on a large scale. These models are a subset of machine learning and are based on neural networks, particularly a class known as transformers.

in the future by following different management principles. AI and ML technology can potentially improve military decision-making at all levels of command, but broader operationalisation of this concept will require additional experimentation and testing to build necessary trust. Operational AI, despite some uncertainties and limitations, could relatively soon meet the primary requirement of avoiding tactical mistakes by identifying a system's critical state, which requires a particular interest and resolution (In the realm of military operations, this includes detecting adversary movements in time to prevent surprise attacks on friendly forces). The evolution of AI in the military will contribute to civilian progress and vice versa. Similar to hybrid warfare, AI will likely become omnipresent, blurring the boundaries between application domains.

The ongoing need for agility and development of rapid counter-measures will drive innovative and flexible solutions to the adaptive serial production lines, logistics and supply chains, software development, predictive diagnostics, and real-time identification of weak points in the field (utilising technologies such as 3D Printing and Additive Manufacturing). This will also affect many aspects of the civilian domain, such as the development of in-home, portable and adaptive production systems, including advanced self-diagnostics and digital-twin area evolution. There is a general consensus that cybersecurity and cyber warfare will become crucial for future defence and civilian applications. The future hybrid conflict will target the civilian infrastructure with a similar intensity as military forces and assets. Thus, cyber warfare capabilities will be a crucial component of military operations, mainly targeted to the critical sectors of the military systems, like communication infrastructure, networks, databases, and cloud services.

Autonomous military robots (UAVs, UGVs, and UUVs) have undergone a dynamic and inevitable technological evolution, showing their clear potential to outperform humans in all combat functions and domains. This will lead to an explosion of potentially new or improved contemporary civilian applications in industry, agriculture, security, medicine, transportation, sports, and leisure.

Quantum computing and communications have the potential to revolutionise the military and civilian sectors through advancements in secure communication, computing power, and encryption. Although it is at an early stage, significant progress is expected in this area within the next few years. This could introduce dramatic technological breakthroughs and unimaginable opportunities, such as solutions for very complex tasks and safe and real-time intergalactic communication.

Space capabilities and the development of anti-satellite and space defence weapons, satellites, and space technology for communication, surveillance, and navigation are expanding rapidly and will continue to be essential for military operations over the next decade.

Hypersonic weapons provide new precision attack and defence capabilities, posing unique challenges for existing defence systems. DEWs could outperform this technology in countermeasures and significantly degrade its potential. DEWs provide precision attack and defence capabilities against other threats like drones

and aircraft, presenting a vast potential for future warfare, so that enormous effort is dedicated to this area.

Advanced materials and nanotechnology allow the creation of more robust and lighter military equipment, from personal armour to vehicles, and present one of the most intense development fields in the civilian domain. This field possesses enormous potential, and development in this area is a logical outcome of military and civilian needs in almost all domains. Also, in the modern world, the military, industry, space, electronics, and other domains will rely substantially on advanced batteries and new power generation methods for their energy needs. This area is growing dynamically and sets a critical operational limit within different domains.

Because recent experiences demonstrate that the cyber domain is being heavily exploited by civilian population, it is reasonable to assume that future wars will become more hybrid and interwoven with the civilian sector. This leads to closer cohesion regarding dual-use technologies and production benefits, which could be interconnected so deeply that the functionality within a particular domain will be driven or defined only by SW features, like those in many technological components today (e.g. car engines). Although it is expected that these domains will advance simultaneously, the world will likely never return to the Cold War era when "doctrine pulled technology". Therefore, dual-use technologies are likely to be more closely fused, and the potential benefits of successful developments in one domain will immediately appear in others.

A critical step in the dynamic evolution of advanced technologies within armies is establishing trust in advanced automation (autonomy), including in AI/ML and other EDT-based technologies. This is a crucial and complex challenge for all armies worldwide. It requires a multifaceted approach, addressing technical reliability, ethical governance,[79] user training, involvement in the development process, and positive experiences/examples (i.e. demonstrating successful instances where advanced technologies have enhanced mission effectiveness, reduced casualties, or aided in humanitarian efforts). In conclusion, it is important to note that extreme conservatism regarding the implementation of cutting-edge technology will significantly reduce the military's ability to respond to rapidly developing operating environment issues. This could have lethal repercussions.

79 Chameau, 2014.

References

Ackerman, E. (2022) 'DARPA's RACER Program Sends High-Speed Autonomous Vehicles Off-Road', *IEEE Spectrum*, 27 January 2022. [Online]. Available at: https://spectrum.ieee.org/darpa-robot-racer. (Accessed: 15 January 2024).

Ahokangas, P., Aagaard, A. (eds.) (2024) *The changing world of mobile communications: 5G, 6G and the future of digital services*. Cham: Palgrave Macmillan; https://doi.org/10.1007/978-3-031-33191-6.

Bikos, A.N., Kumar, S.A.P. (2022) 'Enhancing space security utilizing the blockchain: Current status and future directions', *Institute of Electrical and Electronics Engineers Inc.*, pp. 77–82; https://doi.org/10.1109/WiSEE49342.2022.9926843.

Billing, D.C., Fordy, G.R., Friedl, K.E., Hasselstrøm, H. (2020) 'The implications of emerging technology on military human performance research priorities', *Journal of Science and Medicine in Sport*, 24(10), pp. 947–953; https://doi.org/10.1016/j.jsams.2020.10.007.

Black, J., Lucas, R., Kennedy, J., Hughes, M., Fine, H. (2024) *Command and Control in the Future: Concept Paper 1: Grappling with Complexity*. Santa Monica, CA/Cambridge, UK: Rand Corporation.

Blakley, C.T., Li, L.W., Eakman, G., Baker, B.C. (2022) 'Engineering resilient systems cloud computing architecture (ECCA): A collaborative and secure analysis framework', *Journal of Defense Modeling and Simulation*, 19(3), pp. 299–311; https://doi.org/10.1177/1548512920960539.

Chameau, J.L., Ballhaus, W.F., Lin, H.S. (eds.) (2014) *A Framework for Addressing Ethical, Legal, and Societal Issues*. Washington, DC: National Academies Press.

Cone, P. (ed.) (2019) 'Assessing the influence of hypersonic weapons on deterrence', *Future Warfare Series No.* 59, *USAF Center for Strategic Deterrence Studies, Air University*, June 2019. [Online]. Available at: https://purl.fdlp.gov/GPO/gpo139495 (Accessed: 1 January 2024).

Dahdal, S., Poltronieri, F., Tortonesi, M., Stefanelli, C., Suri, N. (2023) 'A Data Mesh Approach for Enabling Data-Centric Applications at the Tactical Edge', *Institute of Electrical and Electronics Engineers, Inc.*; https://doi.org/10.1109/ICMCIS59922.2023.10253568.

De Mattia, S. (2022) 'Modelling and Simulation for Behavioral Codes of Robotics and Autonomous Systems' in Mazal, J., Fagiolini, A., Vasik, P., Turi, M., Bruzzone, A., Pickl, S., Neumann, V., Stodola, P. (eds.) *Modelling and Simulation for Autonomous Systems*. Cham: Springer, pp. 180–190; https://doi.org/10.1007/978-3-030-98260-7_11.

Del Monte, L.A. (2021) *War at the speed of light: Directed-energy weapons and the future of Twenty-First Century warfare*. Lincoln, NE: Univeristy of Nebraska Press; https://doi.org/10.2307/j.ctv1f70m1m.

Durlach, PJ., Lesgold, A.M. (eds.) (2012) *Adaptive Technologies for Training and Education*. Cambridge: Cambridge University Press; https://doi.org/10.1017/CBO9781139049580.

Gent, E. (2020) 'Watch a swarm of drones fly through heavy forest – while staying in formation', *Science*, 16 December 2020. [Online]. Available at: https://www.science.org/content/article/watch-swarm-drones-fly-through-heavy-forest-while-staying-formation (Accessed: 5 January 2024).

Govindaraju, V, Raghavan, V., Rao, C.R. (eds.) (2015) *Big data analytics*. 1st edn. Vol. 33. Amsterdam: Elsevier.

Gregg, H.S. (2016) 'The Human Domain and Influence Operations in the 21st Century', *Special Operations Journal*, 2(2), pp. 92–105; https://doi.org/10.1080/23296151.2016.1239978.

Guillaume, D., Samuel, D., Franck, B., Pol, M., Frédérique, L.L. (2019) 'Composite propeller in marine industry: First steps toward a technological breakthrough', *Institute of Electrical and Electronics Engineers Inc.*; https://doi.org/10.1109/OCEANSE.2019.8867439.

Hagos, D.H., Rawat, D.B. (2022) 'Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives', *Sensors*, 22(24); https://doi.org/10.3390/s22249916.

Hahn, G.L., Tsotsis, T.K. (2019) 'Rapid high-performance molding (RAPM) for small parts', *Society for the Advancement of Material and Process Engineering*; https://doi.org/10.33599/nasampe/s.19.1388.

Hallaq, B. et al. (2017) 'Artificial intelligence within the military domain and cyber warfare', *Curran Associates Inc.*, pp. 153–156. [Online]. Available at: https://wrap.warwick.ac.uk/id/eprint/94297/1/WRAP-artificial-intelligence-within-military-domain-cyber-warfare-Hallaq-2017.pdf (Accessed: 5 January 2024).

Hutcheon, A. (2021) 'Biotechnology, Human Enhancement and Human Augmentation: A Way Ahead for Research and Policy', *NATO*, December 2021. [Online]. Available at: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc386/p814643_A1b.pdf (Accessed: 3 January 2024).

Johnson, J. (2023) 'Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age', *Defence Studies*, 23(1), pp. 43–67; https://doi.org/10.1080/14702436.2022.2102486.

Krelina, M. (2021) 'Quantum technology for military applications', *EPJ Quantum Technology*, 8(1); https://doi.org/10.1140/epjqt/s40507-021-00113-y.

Krichen, M., Ammi, M., Mihoub, A., Almutiq, M. (2022) 'Blockchain for modern applications: A survey', *Sensors*, 22(14); https://doi.org/10.3390/s22145274.

Kuptel, A., Williams, A. (2014) 'Policy Guidance: Autonomy in Defence Systems', *Supreme Allied Commander Transformation HQ*, 29 October. [Online]. Available at: http://dx.doi.org/10.2139/ssrn.2524515 (Accessed: 9 January 2024).

Liu, G.D. et al. (2021) 'Military medical research on internal diseases in modern warfare: new concepts, demands, challenges, and opportunities', *Military Medical Research*, 8(20); https://doi.org/10.1186/s40779-021-00313-8.

Loganathan, A., Ahmad, N.S. (2023) 'A systematic review on recent advances in autonomous mobile robot navigation', *Engineering Science and Technology, an International Journal*, 2023/40; https://doi.org/10.1016/j.jestch.2023.101343.

Lovalekar, M., Sharp, M.A., Billing, D.C., Drain, J.R., Nindl, B.C., Zambraski, E.J. (2018) 'International consensus on military research priorities and gaps – Survey results from the 4th International Congress on Soldiers' Physical Performance', *Journal of Science and Medicine in Sport*, 21(11), pp. 1125–1130; https://doi.org/10.1016/j.jsams.2018.05.028.

Mamalis, A.G. (2019) 'Advanced manufacturing under impact/shock loading: Principles and industrial sustainable applications', *Association of American Publishers*, 2019/13, pp. 13–24; https://doi.org/10.21741/9781644900338-3.

Manso, M. et al. (2023) 'IoT in Coalition Federated Operations: Multi-national C2 Integration and Technical Interoperability Experiments', *Institute of Electrical and Electronics Engineers Inc.*; https://doi.org/10.1109/MILCOM58377.2023.10356285.

Manson, K. (2020) 'China and the US: readying for war in space', *Financial Times*. [Online]. Available at: https://www.aspresolver.com/aspresolver.asp?MARC;5144632 (Accessed: 7 January 2024).

Mazal, J., Procházka, J., Zezula, J., Procházka, D. (2022) 'Využití modelování na simulace v procesu optimalizace výstavby Ozbrojených sil České republiky' [The use of modelling on simulation in the process of optimization of the construction of the Armed Forces of the Czech Republic], Vojenské rozhledy, 31(4), pp. 140–158. [Online]. Available at: https://vojenskerozhledy.cz/kategorie-clanku/vystavba-ozbrojenych-sil/modelovani-simulace-optimalizace-vystavba (Accessed: 1 January 2024).

Mazal, J., Bruzzone, A., Kutej, L., Scurek, R., Zlatnik, D. (2020) 'Optimization of the ground observation', *Proceedings of the 22nd International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation* (HMS 2020), pp. 71–74; https://doi.org/10.46354/i3m.2020.hms.011.

Mazal, J., Bruzzone, A., Turi, M., Biagini, M., Corona, F., Jones, J. (2019) 'NATO Use of Modeling and Simulation to Evolve Autonomous Systems' in Mittal, S., Tolk, A. (eds.) *Complexity Challenges in Cyber Physical Systems: Using Modeling and Simulation (M&S) to Support Intelligence, Adaption and Autonomy*. Hoboken, NJ: John Wiley and Sons Inc.; https://doi.org/10.1002/9781119552482.ch3.

NATO (2018) 'Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018' *Press Release* (2018)074, Brussels, 11 July 2018. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_156624.htm. (Accessed: 5 January 2024).

NATO EDT's (2024) 'Emerging and disruptive technologies', 8 August 2024. [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_184303.htm. (Accessed: 18 January 2024).

Okyay, C. (2023) 'Emerging and Disruptive Technologies for Military and Defence', *Linkedin*, 29 May 2023. [Online]. Available at: https://www.linkedin.com/pulse/emerging-disruptive-technologies-military-defence-cem-okyay (Accessed: 15 January 2024).

Ravi, V., Cherukuri, A.K. (eds.) (2021) *Handbook of Big Data Analytics: Applications in ICT, Security and Business Analytics, Vol. 2*. London: Institution of Engineering & Technology; https://doi.org/10.1049/PBPC037G.

Salomon, J.M. (2022) 'Public-Private Partnerships and Collective Cyber Defence', *NATO CCD COE Publications*, May 2022, pp. 45–63; https://doi.org/10.23919/CyCon55549.2022.9810912.

Salor, L.C., Baeza, V.M. (2023) 'Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications', *Telecom*, 4(4), pp. 709–731; https://doi.org/10.3390/telecom4040032.

Sarcia, S.A., Colo, G. (2023) 'Organizing structures and information for developing AI-enabled military decision-making systems', *Institute of Electrical and Electronics Engineers Inc.*, pp. 455–460; https://doi.org/10.1109/TechDefense59795.2023.10380925.

Scharre, P. (2019) *Army of none: autonomous weapons and the future of war*. New York, NY: W.W. Norton & Company.

Scharre, P. (2023) *Four Battlegrounds: Power in the Age of Artificial Intelligence*. 1st edn. New York, NY: W.W. Norton & Company.

Suárez, E.J.A., Baeza, V.M. (2023) 'Evaluating the Role of Machine Learning in Defense Applications and Industry', *Machine Learning and Knowledge Extraction*, 5(4), pp. 1557–1569; https://doi.org/10.3390/make5040078.

Surdu, J., Kittka, K. (2008) 'The Deep Green concept', *MSIAC Journal*, 3(3), pp. 4–12. [Online]. Available at: https://apps.dtic.mil/sti/tr/pdf/ADA500860.pdf (Accessed: 5 January 2024).

Tarraf, D.C., Gilmore, J.M., Barnett, D.S., Boston, S., Frelinger, D.R., Gonzales, D., Hou, A.C., Whitehead, P. (2022) 'An experiment in tactical wargaming with platforms enabled by artificial intelligence', *Journal of Defense Modeling and Simulation*; https://doi.org/10.1177/15485129221097103.

Thakker, R., Alatur, N., Fan, D.D., Tordesillas, J., Paton, M., Otsu, K., Toupet, O., Agha-mohammadi, A. (2021) 'Autonomous Off-Road Navigation over Extreme Terrains with Perceptually-Challenging Conditions' in Siciliano, B., Laschi, C., Khatib, O. (eds.) *Experimental Robotics*. Cham: Springer, pp. 161–173; https://doi.org/10.1007/978-3-030-71151-1_15.

United States Government Accountability Office (2023) 'Directed energy weapons: DOD should focus on transition planning: report to congressional committees' *Report to Congressional Committees*, April 2023. [Online]. Available at: https://purl.fdlp.gov/GPO/gpo221259 (Accessed: 14 January 2024).

Volkov, K.N. (2023) *Hypersonic and supersonic flight: advances in aerodynamics, materials, and vehicle design*. IntechOpen; https://doi.org/10.5772/intechopen.104045.

Wasim, M.S., Habib, S., Amjad, M., Bhatti, A.R., Ahmed, E.M., Qureshi, M.A. (2022) 'Battery-Ultracapacitor Hybrid Energy Storage System to Increase Battery Life Under Pulse Loads', *IEEE Access*, 2022/10, pp. 62173–62182; https://doi.org/10.1109/ACCESS.2022.3182468.

Williams, A., Scharre, P. (eds.) (2015) *Autonomous Systems: Issues for Defence*. Norfolk, VA: NATO Allied Command Transformation. [Online]. Available at: https://www.researchgate.net/publication/282338125_Autonomous_Systems_Issues_for_Defence_Policymakers (Accessed: 5 January 2024).

Woods, D.L., Wyma, J.M., Yund, E.W., Herron, T.J., Reed, B. (2015) 'Factors influencing the latency of simple reaction time', *Frontiers in Human Neuroscience*, 2015/9; https://doi.org/10.3389/fnhum.2015.00131.

Artificial intelligence is growing dozens of times faster than Moore's Law (2020) *Gigazine*, 7 July 2020. [Online]. Available at: https://gigazine.net/gsc_news/en/20200707-ai-training-cost-moores-law/ (Accessed: 13 January 2024).

Chinese Scientists Unveil Breakthrough 'Low-Temperature Plasma Shield' for Military Defense (no date) *Impact Lab*. [Online]. Available at: https://www.impactlab.com/2024/01/23/chinese-scientists-unveil-breakthrough-low-temperature-plasma-shield-for-military-defense/ (Accessed: 25 January 2024).

A graph showing how artificial intelligence (AI) has overtaken humans and overtaking them is like this (2017) *Gigazine*, 3 July 2017. [Online]. Available at: https://gigazine.net/gsc_news/en/20170703-ai-progress-measurement/ (Accessed: 5 January 2024).

Chapter 7

Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies

János Székely

Abstract

This chapter aims to address the problem presented by governance regimes applicable to the dual (civilian and military) use of emerging and disruptive technologies such as artificial intelligence and biotechnology. The author first examines the definition of "dual use" as it emerges from various unilateral and multilateral governance instruments. As several definitions currently coexist, "dual use" is found to constitute a fuzzy notion, requiring clarification in further regulation and application. The major regimes governing dual-use technology proliferation and trade are presented with an emphasis on the role of securitisation in determining the applied regulatory approach and content. The technological and economic rivalry between the United States of America and the People's Republic of China was found to have a defining role in the current transformation of such governance regimes to the detriment of free trade. Subsequently, the problems posed by artificial intelligence, biotechnology, and 5G broadband data transfer were examined in light of dual-use technology regulation, with conclusions presented regarding the future desirable development of the regulatory environment.

Keywords: dual-use, emerging technology, disruptive technology, securitisation, export control.

János Székely (2024) 'Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 309–353. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_7

1. Introduction

1.1. Dual use as a result of technological synergies

Technological and scientific development and warfare are closely associated. Some of the defining inventions of modern life itself, in fields ranging from power generation to medicine, manufacturing to telecommunications, and transportation to data processing, have either been employed during warfare or, quite often, have even been developed[1] specifically with warfare in mind. Thus, some technologies have peaceful and war-like applications simultaneously while requiring little to no adaptation to suit either purpose. These are the situations to which the notion of dual-use technology, in its broadest sense, refers.

The ongoing wars in Ukraine or the Middle East allow us to observe, for example, the deployment[2] of small, toy-like unmanned aerial vehicles ("drones" in common parlance, sometimes abbreviated as UAS in the case of light-weight systems, although henceforth we will refer to them as UAVs) during combat operations.[3] Many of these platforms, unlike larger, military-grade UAVs, were initially designed for hobbyists interested in amateur aerial photography rather than for military use. Adding simple mounts for ammunition to be released over the heads of enemy forces converts what was once conceived of as little more than high-end toys, into weapons of war.

In cases when such dual use occurs, a synergy of different technologies, building on various specialised items and knowledge, is indispensable: to construct an improvised combat UAV, an off-the-shelf product must be modified and reprogrammed by capable personnel. It would not function without advanced telecommunication support (possibly access to the Internet, or some other way of conveying commands and transmitting flight telemetry, as well as image data, likely also requiring electronic countermeasures to evade hostile jamming efforts), access to a global navigation system, or the microprocessors, cameras, remote controllers, screens, antennas, motors, and actuators assembled as a "package" (albeit with a purpose other than war), which permit effective use of the toy-turned-weapon in combat by the operator.

This case is instructive in several respects: First, it demonstrates that technologies thought of as generic or civilian are often of dual use. Second, it shows that the regulation of such technologies, especially by rules intended to prevent their proliferation or hostile use, is difficult to accomplish and may affect free trade and civilian technological development. Third, it shows that whenever we consider dual-use "technologies" in the strict sense, we cannot ignore the categories from which such dual use stems, simply because the technology itself is a result of a synergy

1 Brunk and Jason, 1981, pp. 437–455.
2 Puranik, 2021, pp. 33–52.
3 Thompson, 2024.

(a self-enforcing interaction) between *specialised knowledge* (such as that gained by research and experimentation) and *artefacts*, or *items* (ranging from raw materials, to manufactured – corporeal – goods).[4] Therefore, dual-use knowledge, items, and technologies should all be considered as separate objects of regulation. I shall nonetheless examine them together, as references to dual-use technology oftentimes include not just "technology" in the proper sense of the word, but also knowledge, and items (components) utilised in its makeup.

1.2. The "grey zone" of dual-use technologies

Some knowledge, items, and technologies, such as those whose purpose is evidently the construction of weapons of mass destruction (WMDs), weapon systems, or other possibly destructive end uses (e.g. the aptitudes of some nuclear scientists, rockets and jet engines, highly enriched or weapons-grade fissile materials, reactor containment vessels, precursor chemicals, pathogens, avionics equipment, advanced aerospace alloys, radars and targeting systems, directed energy systems, specialised machine tools, etc.) present obvious dangers, and their identification and strict regulation poses less of a challenge. These fall into a "black zone" of knowledge, items, and technologies (mostly dealt with by non-proliferation conventions and weapons embargos) with clearly defined edges or limits for some obviously destructive purpose.

The difficult question for experts, regulators, and industry alike is how to define and regulate items, technologies, and knowledge that do not fall neatly into this category, but are part of a "grey zone", being (mostly) employed in the civilian sector, or with only marginal obvious significance for warfare, unless some destructive synergies are created, such as the ones which gave rise to the improvised combat UAV. Clearly, weapon systems cannot be reasonably considered as having a "dual use": their single envisaged use is combat itself. Therefore, these will not form the object of my analysis, as they are mainly subject to rules on *stricto sensu* arms control.

Thus, the subject matter of my study shall be constituted by the "grey zone" items, technologies, and knowledge, the proliferation of which, even for civilian use, may result in nefarious applications. This is because this "grey zone" is the one that also includes many of the most significant technological developments for civilian use, and which presents grave implications for global economic interconnectedness, including technological interdependency.

While underregulating dual-use technologies poses significant risks, overregulation or abusive enforcement of regulation may also result in costs, which may have a chilling effect on the development of certain technologies, as during the allocation of funding, such extant or future limitations on their potential markets will be considered. Various regimes regarding dual-use technologies seek mainly to balance national security and national interest concerns with those of business: a high regard

4 For this categorisation, see: Forge, 2010, pp. 112–115.

for national security may be paired with a low or high regard for national business interests, and consideration may also be granted to national business interests as part of national security concerns.[5]

One other problem for national security, which is rarely voiced, but should not be ignored when studying the problems posed by dual-use technology regulation, is the "conversion" of dual-use knowledge, items, and technologies,[6] which permits some flexibility in the transfer of resources between enterprises with a focus on defence or on civilian implementation as desirable. In this manner, defence spending during low-threat periods may be reduced without losing the capability to re-employ resources for defence if needed.[7] Such conversion has the added benefit of camouflaging defence spending, as exemplified by the development of UAV technology using European Union (EU) research funding (e.g. Horizon 2020 projects), through consortia with a hybrid (state and private) structure and also a hybrid (both civilian and military) purpose, which constitute a nascent "European Industrial Military Complex" as a response to recent changes in the strategic environment and the defence needs of EU member states.[8]

1.3. Securitisation as the common element of current dual-use technology regulation

In the field of dual-use technologies, various regulatory regimes aim to address two problems. The difficulties of this endeavour are usually summed up by the 'dual-use dilemma' and the 'dual-use security dilemma'.[9] The former refers to the risk of intentional or accidental misuse (including unintended military use) of knowledge, items, or technology in general and is mainly treated in ethical codes, as well as domestic and international regulatory regimes which aim to prevent misuse. The latter constitutes a behavioural pattern between two actors, where the second fears that the first will develop or acquire dual-use knowledge, items, or technologies to utilise them for military purposes, and aims to prevent such an acquisition. In this second dilemma, every measure one actor takes is considered to have an offensive purpose by the other, leading to a spiral of ever-stricter responses and counter-responses with potentially devastating effects on regional and global trade as well as technological development.

The regulation of dual-use knowledge, items, and technologies may, even without any hostile relations between economic actors, constitute a pretext for erecting tariff-like barriers, thus excluding some actors from markets and resulting in trade policies instituted to create a civilian industrial base, which can then be turned to

5 Seyoum, 2017, pp. 695 et seq.
6 Brandt, 1994, pp. 365 et seq.
7 See: Skolnikoff, 2008, pp. 42–47.
8 Martins and Küsters, 2019, pp. 280 et seq.
9 Lupovici, 2021, pp. 260–263.

war-like purposes.[10] Such policies may also be weaponised as a tool for trade wars aimed at the economic and political containment of not just real adversaries but also economic competitors.

Numerous theories have been proposed to explain the effects of dual-use technology regulations on trade. They recognise the economic impact of such regimes and that they may be implemented solely for their economic effects, including restrictions on free trade.[11] Markets, especially those in the economic spheres of influence of great powers, may be nudged, or outright coerced to only obtain technology from some suppliers, while competition from entities deemed to be "hostile" may be severely restricted. Such theories, widely referred to as economic securitisation, imply that by designating a given domain as being of existential importance within a political unit (i.e. a state or an alliance system) and viewed from the perspective of the common values of that political system, such a domain may be brought under a regulatory regime specific to urgent threats: it may be regulated by means and methods specific to extraordinary rather than ordinary legislation.[12] In simple terms, economic securitisation means that states or alliance systems consider competition from other states or alliance systems with different values or different geopolitical interests as a hostile act, or at the very least as a long-term threat in and of itself, which must be countered by regulatory means specific to (armed) conflicts. These means may include restrictions on trade and technology transfer as well as other measures to stunt the development of the perceived adversary.

The securitisation of dual-use knowledge, items, and technology poses several problems. The primary issue, which must be considered pivotal to future regulation, is whether, by implementing extraordinary measures, the political entity in which this phenomenon occurs (e.g. Western democracies) creates a counterproductive environment for its own economic development, resulting in the re-establishment of isolated geopolitical blocks to the detriment of interconnectivity. Securitisation, in its extreme manifestation, may even result in the fragmentation of scientific progress, especially when, as proposed,[13] even institutions of higher education should observe measures to prevent the undesired transfer of dual-use knowledge, items, and technologies. Tailoring free-trade regimes set forth in various agreements to curtail dual-use technology transfer outside a given alliance structure is also an increasing practice.[14] All these considerations must be addressed concurrently to understand the impact of dual-use technology regimes in the military, civilian, and specifically, the economic and trade fields.

Owing to such considerations, defining the conceptual limits of dual use and the scope of regimes that impose limits on dual-use knowledge, items, and technologies

10 See: Blanken and Lepore, 2024, pp. 192–205.
11 Fuhrmann, 2008, pp. 645–649.
12 Buzan and Wæver, 2009, p. 265. For further details on securitisation theory, see: Taureck, 2006; Floyd, 2007; Stritzel, 2007.
13 See: Gearon, 2017; Gearon and Parsons, 2019.
14 Klaus, 2003, pp. 120–129.

is indispensable. Yet, partly due to the diversity of such regimes, manifested both in sources of soft law, such as scientific ethics codes, and hard domestic and international law instruments, such as acts of legislation or international conventions, and partly due to the diversity of meanings in which "dual use" is utilised, such a definition is elusive.

The fields in which the dual-use problem has arisen are growing in number as various disruptive technologies (such as biotechnology, artificial intelligence, and quantum computing) have emerged from the synergy of new scientific knowledge, novel materials, and other items as well as previous technologies. Therefore, considering the security and economic implications of restrictions imposed owing to the possible dual use of disruptive new technologies, such limitations must be subject to analysis, which I will undertake in the following sections.

This chapter considers dual-use technology regulation mainly from the perspective of technological development and transfer of technology to avoid over-extending the scope of this enquiry. Due to the breadth of the field of regulation, in a context of ever-increasing securitisation of geoeconomic competition, this study cannot offer a comprehensive view of all the relevant regulatory regimes that may affect dual-use technologies. Therefore, my enquiry is limited mostly to export controls, where the dual-use dilemma is present in the sources of soft law, black letter law, and administrative practices. For this reason, I shall specifically exclude – apart from minor references – from the object of this study the problems of foreign investment screening, which is not specifically regulated by major international instruments, and where the relevant EU regulation[15] has been enacted only relatively recently. This regulation realised only partial harmonisation when creating the EU Investment Screening Mechanism (which focuses specifically on information sharing between the member states, as well as between them and the European Commission, and transparency and non-discrimination), and left the most significant part of setting up and operating domestic investment screening regimes to member states (with the marginal positive effect that some member states that did not operate such screening were induced to create these mechanisms).[16] Consequently, the possible interactions between measures taken to prevent access to dual-use technology by making use of foreign direct investment oversight[17] against potential adversaries and export controls will not be analysed separately.

15 *Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (consolidated text)*, 2019.

16 Bauerle-Danzman and Meunier, 2024, pp. 8–9, 14–15.

17 See: Zwartkruis, 2024.

2. Defining dual use

Defining dual use as referring to knowledge, items, or technologies is fiendishly difficult. Determining the meaning of dual use as an expression constitutes just one layer of the complexity involved. This is because dual-use concepts in sources of hard or soft law, legal (and ethics) literature, and doctrine are by no means unitary; in fact, there exist numerous framings of this notion in both normative instruments and the relevant literature.[18] Some of these conceptually overlap.

Originally, the term "dual use" was clearly meant to achieve the delineation of technologies that may be turned to military or civilian purposes alike, from those (few) which did not pose such risks; this meaning was however superseded with the advent of legal instruments aimed at ensuring non-proliferation of various technologies, especially the prevention of terrorism, through export controls.[19] In this sense, military use was essentially supplanted by malevolent, destructive, or illegal use.[20]

One possible model for the historic transformation of the concept of dual use was charted by Rath et al., who considered national and international non-proliferation and antiterrorism instruments according to the following scheme:

1. dual use in the meaning of a concomitant, i.e. dual civilian, and military purpose for the regulated knowledge, item, or technology complemented by the notions of benevolent or malevolent purpose, when discussing dual use in anti-terrorism, or anti-criminal contexts (with an added distinction between accepted use by allies, and unaccepted use by non-allies) – this concept is present in both national and international, multilateral instruments,
2. dual use, as taken in the above-mentioned civilian–military (or law-enforcement) as well as benevolent–malevolent dichotomies, complemented by a specific meaning of benevolent, or malevolent purpose understood in the context of human rights protection (i.e. the propensity for an end-use of proscribed knowledge, items or technology in order to restrict exercise of, or infringe on human rights) – this concept is mostly present in national (and regional), unilateral instruments,
3. dual use in the meaning of peaceful and non-peaceful purpose of the regulated knowledge, item or technology, a situation encountered in the non-proliferation regimes specifically designed to prevent the spread of weapons of mass destruction (WMDs) – this meaning is usually found in multilateral instruments,
4. dual use in the context of biosecurity oversight, where instead of the traditional dichotomies mentioned above (which consider the – sometimes

18 See: Rath, Ischi and Perkins, 2014; Miller, 2018; Sánchez-Cobaleda, 2022.

19 Rath, Ischi and Perkins, 2014, p. 770.

20 For the possible use categories of technologies deemed as possibly of dual use, including political use for restricting basic freedoms, and the analysis of the difficulties presupposed by defining such categories, see: Mahfoud et al., 2018.

presumed – purpose or use-case), the risks posed by the regulated knowledge or item is considered, especially regarding whether it could be wilfully, or inadvertently diverted from its original purpose, thus giving rise to a risk-based approach, which transcends the known or presumed intentions of the user – this approach is specific to ethics guidelines in scientific research.[21]

Regarding the presence of the notion of dual use in various major international instruments, it has been shown[22] that the Treaty on the Non-Proliferation of Nuclear Weapons[23] only refers to dual use indirectly (when mentioning fissile – "fissionable" – materials); the Biological Weapons Convention[24] refers to the purpose of use of certain biological agents, an approach that is mirrored by the Chemical Weapons Convention[25] (however, the latter also includes schedules listing substances that are to be considered as being of potential dual use), while UN Security Council Resolution 1540 (2004) employs the notion of dual use materials only implicitly, with reference to proscribed materials lists.[26] Other – mostly non-binding (soft law), even if regularly adhered to – instruments, such as the Nuclear Suppliers Group Guidelines,[27] the Missile Technology Control Regime Guidelines,[28] and the Australia Group Guidelines and Common Control Lists[29] employ the notion of "dual use" explicitly, usually to refer to the substances, items, technology, and software included in specific proscription lists.[30] Among international soft-law instruments, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies[31] stands out (as the successor regime to the previous Coordinating Committee for Multilateral Export Controls, or COCOM, arrangement), as its rules attempt to define dual use by separating military and nonmilitary utilisation of the various items to which it refers.[32]

21 Rath, Ischi and Perkins, 2014, pp. 771–779. A situation related to this last meaning of the notion of dual use may also be conceived in the case of artificial intelligence and other disruptive technologies (e.g. nanotechnology, quantum computing, etc.) which by their possibly world-altering effects would only be comparable to biotechnology, but which, due to their theoretical nature, are as of yet unregulated or underregulated.

22 Rath, Ischi and Perkins, 2014, pp. 774–777; Sánchez-Cobaleda, 2022, pp. 77–95.

23 *Treaty on the Non-Proliferation of Nuclear Weapons*, 1968.

24 *The Biological Weapons Convention*, 1972.

25 *Chemical Weapons Convention*, 1993.

26 'Related materials: materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery'. UNODA, 2004.

27 *Nuclear Suppliers Group Guidelines*, no date.

28 *Missile Technology Control Regime Guidelines*, 2023.

29 The Australia Group, no date b.

30 Rath, Ischi and Perkins, 2014, pp. 771–777; Sánchez-Cobaleda, 2022, pp. 77–95.

31 *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, 1995.

32 Rath, Ischi and Perkins, 2014, p. 774; Sánchez-Cobaleda, 2022, pp. 77–95.

Thus, the concept of dual use is, apparently, inextricably linked to what have been referred to as 'purpose concepts',[33] in fact, dichotomies of "desirable" and "undesirable" purposes, and which may be summarised as follows: a civilian or a military purpose, a benign (non-destructive) or a malevolent (destructive) purpose, a peaceful or a non-peaceful purpose, a legitimate or an illegitimate purpose (from the perspective of national security and human rights), and finally a "good" military or a "good" civilian purpose, as opposed to "bad" civilian and "bad" military purposes (mostly significant in the case of technologies with important civilian uses).

It should be emphasised here that while the literature recognises the case of dual use, where such use may be inadvertent (i.e. in the form of risk-based ethical regulation), this cannot be comfortably squared with any of the above-mentioned dualist categories, which implicitly assume the existence or possibility of a purpose, that is, are based on the presumed intentions of the user.

This, in turn, renders the concept of dual use vulnerable to misconstruction based on the regulator's intrinsic perspective, instead of on any set of objective criteria. Thus, the risk of dual use may at times just be in the eye of the beholder, that is, it may depend more on irrational elements than on any objective criterion.[34]

This conclusion underscores one of the major issues that I would like to address in this chapter: In the regimes set up to regulate dual-use knowledge, items, and technology, the casuistic approach runs rampant. Such a method of regulation, even of soft-law norms such as ethics codes, is particularly problematic in the case of scientific knowledge already gained and cutting-edge research, where in both life sciences and artificial intelligence, the notion of 'dual-use research of concern'[35] has evolved, just as dual use previously did, very much under the radar of legal scholarship.

The complementary concepts of knowledge, items, and technology are also somewhat problematic, as they may include tangible items or entire technologies (materials, plans, research results, microprocessors, UAVs, etc.) but almost always present an intangible component in the form of education, training, and know-how.[36]

Thus, the conceptual systematisation of rules pertaining to dual-use knowledge, items, and technologies is an evident necessity. In the international arms control law literature, a fourfold system of factors has been developed to determine if an item should be proscribed (including as being dual-use), which may also be readily applied to dual-use technology regulation in its entirety:

> Whether or not an authorization for the export of an item is required will, in general, be determined by answering the "what", "where", "who", and "how" questions. What

33 Rath, Ischi and Perkins, 2014, pp. 779–783; Sánchez-Cobaleda, 2022, pp. 77–95.

34 This phenomenon is present in the 'I'll know it when I'll see it' doctrine developed by the Supreme Court of the United States in the case of *Jacobellis v. Ohio* (1964), when it was used to avoid providing a detailed definition of the concept of "pornography". Gewirtz, 1996, p. 1026; Rath, Ischi and Perkins, 2014, p. 777.

35 Urbina et al., 2022, p. 607.

36 On this problem, see: Katz, 2020; Sánchez-Cobaleda, 2022.

are the product specifications of an item, and do they correspond with a listed item (classification)? Where is an item heading (destination); is that State subject to a sanctions regime? Who is ultimately the user of the item (end-user)? And finally, how will the item ultimately be used (end-use)?[37]

Such a system, when adapted to the regulation of dual-use knowledge, items, and technologies, could be used to summarise and systematise the approaches described above. This tentative systematisation is presented in the following table:

Table 1. Summary of approaches to the various definitions of dual use (author's own).

Context of dual-use definition	Main characteristic of use category	Dual-use character determined according to:	Instruments
Traditional perspective	civilian / military use	end use	national and international (multilateral); binding and non-binding
Positional[38] perspective	use by an ally / use by an adversary	end user, end use	mostly national and regional (e.g. EU) binding instruments
	accepted use / unaccepted use	end use	
Law-enforcement and anti-terrorism perspective	legal use / illegal use	end user, end use	national and international (multilateral), binding and non-binding instruments
Human rights perspective	potential use infringing on human rights	end user, end use	national and regional unilateral instruments

37 Voetelink, 2022, p. 72.

38 What I choose to call a "positional" definition here refers to provisions contingent on the status (position) of an actor. Under such a definition, the very same conduct may be legal when exercised by one actor, and illegal when exercised by another. Such positional rules regularly result from value-system principles (moral, political, and ethical principles) that imbue legal rules with external values (such as states under a rule of law, as opposed to states considered autocracies). These values are sometimes subject to sudden change. See: Kelsen, 1991, p. 115.

Context of dual-use definition	Main characteristic of use category	Dual-use character determined according to:	Instruments
Non-proliferation of WMD perspective	potential nefarious (non-peaceful) use	classification, destination, end user	binding international (multilateral) instruments, national instruments
Biosecurity and life sciences perspective	potential for unethical, risky, or nefarious (non-peaceful) use	classification, end user, end use	non-binding ethics codes

I consider that the concept of dual use as well as all complementary concepts indicated above constitute what is called, including in legal science, a *fuzzy set*, that is, a set whose elements cannot be clearly defined, with some meanings possibly outside the set, as well as inside it, and major conceptual overlaps, depending on subjectively attributed criteria (resulting from the "I'll know it when I'll see it" approach intrinsic to the regulation of the topic).[39] This is a well-known problem in instruments aimed at achieving non-proliferation and arms control, where the use of imprecisely defined notions is both intentional and problematic, not just allowing political manoeuvring, but also inadvertent misunderstanding[40] when it comes to potential dual-use knowledge, items, or technologies subject to the imposed measures.

The creation of a functional normative definition of dual-use technology has also been attempted. In our opinion, the best definition to date was proposed by Forge and is as follows:

> An item (knowledge, technology, artefact) is dual use if there is a (sufficiently high) risk that it can be used to design or produce a weapon, or if there is a (sufficiently great) threat that it can be used in an improvised weapon, where in neither case is weapons development the intended or primary purpose.[41]

The author aptly notes immediately after the definition that 'The judgements about risk and threat are contextual […]. Also, the definition presupposes a system of values that informs the general attitude to weapons production as bad because it provides the means to harm'.[42]

In this way, the subjective complementary content of the definition stands clearly recognised: this definition, and in fact any attempt at a normative definition of dual use, is predicated on first creating a moral framework for acceptable and unacceptable

39 See: Legrand, 1999, p. 238.
40 Bremer-Maerli and Johnston, 2002, pp. 54–56.
41 Forge, 2010, p. 117.
42 Forge, 2010, pp. 117–118.

use that will inherently constitute a value-judgement on the purpose of the user, which in turn presents numerous difficulties.[43] First, there is no universal, all-encompassing definition of dual use that ignores a subjectively defined purpose. Second, the use of purpose-based dichotomies makes divorcing any possible definition from a case-by-case judgement of particular circumstances, and possibly political or economic expediency, rather difficult. Third, this exposes regulatory regimes of dual-use knowledge, items, and technology to securitisation-driven regulation, thereby drawing into the field of such regulation the geopolitical and geoeconomic concerns of the national regulator beyond purely normative (black letter law) content.

A tempting proposition for treating the issue at hand would be to dispense with the notion of dual use, as some international instruments cited above do, and concentrate on the affected knowledge, items, and technology. This solution, however, presents its own risks as it tends to result in "leaky" proscription lists, especially if tailored too tightly around extant information. Therefore, it would exclude emerging disruptive technologies, at least until a periodic review of the lists of proscribed knowledge, items, or technology is duly undertaken, a problem that, as I shall show below, is currently present, especially in the (non)regulation of dual-use artificial intelligence algorithms. Conversely, a general list of proscribed objects would result in stifling trade, even when dual-use risks are minimal or non-existent. Finally, the creation of global and regional governance regimes, complete with institutions that would determine the dual-use potential of knowledge, items, and technologies through a transparent procedure administered by a court or arbitration body, would be desirable. Such proposals merit consideration by national regulators and international organisations.

3. Major regulatory regimes applied to dual-use technologies

Governance and regulatory regimes applied to dual-use technologies can be classified as either *multilateral* or as *unilateral* regimes. The first is characterised by some form of cooperative adoption and enforcement, even if the regime itself is based on soft law, that is, non-binding instruments. The second is based on the national instruments by which the desired export controls are achieved. While unilateral regimes abound in the field of dual-use technology regulation, multilateral regimes have historically proven to be more efficient tools for preventing the undesired proliferation of technology and providing regulatory templates for unilateral regimes.

43 I would also like to note here that the definition seems to ignore forms of non-desirable use, other than military use, even if such forms, including infringements of human rights, result in inadvertent but possible existential risks.

An example of such multilateral solutions and arms control regimes is the well-established element of the international legal order. Binding and nonbinding instruments with the scope of preventing the proliferation or development of WMDs abound and have existed for a considerable amount of time (at least since the 17th century).[44]

Numerous such instruments, especially those adopted beginning in the second half of the 20th century, many of which will be mentioned in this respect in the following, usually contain some provisions regarding dual-use knowledge, items, or technologies, even if the notion of dual use itself is not explicitly mentioned in their text. Their stated aim was to enhance global, regional, and national security by restricting the proliferation of knowledge, items, and technologies that were considered to pose significant risks. Such regimes may manifest themselves in binding multilateral instruments, such as arms control treaties (specifically adopted to defend against the spread of weapons of mass destruction or other types of weapons), export restrictions, and other barriers to trade enacted at the regional level, or unilateral measures.[45]

From the perspective of dual-use knowledge, items, and technologies, the first regime which remains relevant today was the result of the (now – possibly – first) Cold War, namely, the establishment of the Coordinating Committee for Multilateral Export Controls (COCOM) in 1949,[46] with various systems instituted in different forms throughout the Cold War and beyond.[47] The establishment of this first specific regime and its maintenance during the Cold War also occurred with the intention of stunting technological development in countries that were considered hostile to the United States (US).[48] Therefore, it constitutes an eloquent example of a multipurpose regime that serves national security objectives, as well as economic and political leverage in the form of an embargo. The COCOM regime later evolved into the Wassenaar Arrangement,[49] geared initially – in the climate of cooperation and good will that characterised the end of the Cold War – towards preventing technology transfers to "pariah" states that could pose a significant risk to international order. Following this transformation of the COCOM regime, other dual-use technology control regimes continue to aim to restrict technology transfer in the interest of national security as well as to impose embargos and erect other impediments to international development in the interest of major powers.[50]

The most significant multilateral (legally non-binding but generally adhered to) instruments for dual-use technology export control include the Missile Technology Control Regime, the Nuclear Suppliers Group, the Australia Group, and the

44 Davis, 2002, pp. 20–22.
45 For an exhaustive historical list of such regimes, up to the year 2002, see: Grahame, 2002.
46 See: Bown, 2020, pp. 296–298.
47 I shall analyse the notion of dual use in such later regimes, in more detail in the following.
48 See: Hofhansel, 1993.
49 Kim, 2021, pp. 386–387.
50 Davis, 2002, pp. 32–36.

Wassenaar Arrangement. Of these, the last is the most significant, as the other instruments are either not meant to govern dual-use technologies in general terms and remain limited to the fields of nuclear and missile technology, respectively, or (as in the case of the Australia Group, being confined to the governance of chemical and biological technologies[51]) do not explicitly, or even implicitly, consider all emerging and disruptive technologies.

Unilateral export controls constitute regimes instituted at the national or regional level[52] (mostly implemented by significant geopolitical and economic actors or alliances of such actors) to impede the transfer of (dual-use) technology to potential adversaries and competitors. Export controls may result not only from concerns about the proliferation of weapons or technologies that may be weaponised, but also from the intention to contain or sanction potential adversaries, and even to stifle competition. Unilateral regimes may be set up by significant individual technology exporters such as the US and the People's Republic of China (PRC). It is these two exporters' unilateral regimes that I shall present with particular emphasis in what follows, with the proviso that several other major technology exporters, such as some EU member states, also establish significant export control regimes (by adopting national control lists of proscribed items and/or by adhering to the EU Dual-Use Regulation).[53] Before analysing unilateral regimes, however, the most significant international framework for controlling dual-use items, knowledge, and technologies must be discussed.

3.1. The Wassenaar Arrangement

The Wassenaar Arrangement (named for the small town near The Hague where it was signed) was founded in 1995 by the Final Declaration of December 1995[54] and counts among its members 42 technologically advanced countries.[55] It is by far the most significant multilateral regime for regulating dual-use technologies, and the most relevant when it comes to emerging technologies. Based on this arrangement,

51 The Australia Group, no date a.

52 Here I include EU instruments among unilateral export controls as EU norms, which constitute a complex mesh of rules, which intermingle with national export control regimes and are binding upon the member states just as domestic law would be, while the EU, due to its wider scope, cannot be considered an international organisation in the classical sense.

53 E.g. In the year 2023, the Netherlands, Spain, Lithuania, and Finland adopted such national control lists from among the member states of the EU. European Commission, 2024b, pp. 7–8.

54 *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Final Declaration*, 1995.

55 These are as follows: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. Arms Control Association, 2023, n. 1.

the Secretariat instituted by its founding documents publishes and, after considering the feedback from the members, regularly updates the List of Dual-Use Goods and Technologies, and Munitions List.[56] These constitute the proscribed item lists regarding which members agree to institute export controls (implementing a mainly classification-based approach).

Two noteworthy facts should be emphasised. The first is that the Wassenaar Arrangement members include Russia, which in the current security environment is proving extremely problematic when it comes to voluntary compliance,[57] whereas this regime does not include the PRC; the second is that it does not include the EU itself.[58] Even if EU member states are partners in the arrangement, the EU as such is only informally and thus indirectly bound by what is agreed, leaving the content of harmonisation instruments to be determined by a block constituted almost exclusively of members of the arrangement (with the notable exception of Cyprus), without being itself a formal member.

While the arrangement is a sound tool for the control of dual-use technology in general, when it comes to disruptive technologies, it has its shortcomings, as the potential risks and transformative effects of these technologies are not yet known, and many states may desire to progress in developing them. At the same time, the proscribed item lists may not be kept sufficiently up to date to prevent undesired proliferation.

The issue of the PRC's non-participation in the arrangement comes to the fore specifically because of the significant development there related to cyber-surveillance technologies, for which the PRC is also a significant exporter. The arrangement was updated for specific categories of surveillance technologies in 2012–2013, such as systems permitting intrusion into the targeted information technology infrastructure (including mobile telecommunication interception) and internet providers' surveillance tools.[59] However, this was not done with reference to human rights or their possible infringement through the use of mass surveillance, but from traditional defence considerations.

In addition, while the necessity of the arrangement's adaptation to dual-use technologies in general has long been known,[60] and the participating states set out to

> focus on novel or rapidly evolving technologies such as quantum computing, additive manufacturing, suborbital vehicles, advanced sensors, robots and artificial

56 The second volume of these lists is published. For the latest list, see: The Wassenaar Arrangement Secretariat, 2023.

57 The fact that Russia aims to implement dual-use technologies in its military industrial development programmes is quite well known, and even openly stated, and has been so for a long time. See, for example: Bzhilianskaya, 1996.

58 Bown, 2020, p. 298.

59 Kim, 2021, pp. 389–394.

60 Himmelfreundpointner, 2017, p. 65.

> intelligence [considering the Arrangement] as the appropriate forum in which to address trade and security challenges arising from new and emerging technologies,[61]

no notable progress has been made in this regard. However, of the disruptive new technologies, quantum computing is indirectly considered, as the 2023 edition of the Wassenaar Arrangement lists includes technologies that may be utilised to harden or defend cryptography during and after the advent of quantum computing[62] (post-quantum encryption), which would compromise the prime factor-based cryptosystems widely used today.

In addition, while the Wassenaar Arrangement is the gold standard in the domain of multilateral instruments governing the non-proliferation of some dual-use technologies, the technical approach it takes is subject to criticism, as it employs proscribed items lists agreed upon unanimously by the participant states. Such agreements are reached through time-consuming negotiations and therefore may be problematic, as it is necessary to update the arrangement in response to unpredictable advances in disruptive technology, a shortcoming that is already evident with respect to artificial intelligence, as an element of a wider debate[63] on updating the agreement to cover cyber weapons.

Further, the arrangement does not provide for efficient catch-all tools, as it does not result in the adoption of a commonly agreed-upon list of suspicious entities (which would mention end users to whom exports are prohibited) or similar documents, which other mostly unilateral tools utilise. Therefore, while the arrangement is useful as intended against pariah states it is less so against geopolitical adversaries or competitors, a major goal for the development of other dual-use technology regimes, which remain instituted mostly by way of unilateral instruments, even if coordinated at the level of various ad hoc coalitions or alliances.

3.2. The US export control regime

The US operates a complex and comprehensive export control regime[64] comprising several systems or layers of regulation. The rules of the regulatory regime are not limited to what would be considered exports in the common sense of the notion, regarding knowledge, items, or technologies, but also cover so-called deemed exports, i.e. disclosures of information, or release of technologies inside the US to a

61 Griffiths, 2019, p. 4.

62 The Wassenaar Arrangement regulates “post-quantum, quantum-safe or quantum-resistant” algorithms. The Wassenaar Arrangement Secretariat, 2023, p. 95.

63 Ruohonen and Kimppa, 2019, pp. 175–183. The arrangement’s proscribed items list does refer to “military offensive cyber operations” but not specifically to cyber weapons used for surveillance and suppression of human rights.

64 For an overview and critique of this system, see: Congressional Research Service, 2020. See also: Congressional Research Service, 2021.

foreigner, including in situations of academic discourse and scientific communication.[65] One of these layers is constituted by the International Traffic in Arms Regulation (ITAR),[66] which governs weapons and related military-use technology exports (which are not included under the dual-use category). More significant, from the perspective of this chapter, is the Export Authorization Regulations (EAR),[67] through which the Bureau of Industry and Security (BIS) of the US Department of Commerce historically regulated less sensitive technology (not evidently destined for military use).[68] This historic and somewhat limited scope of regulation has been extensively revised since 2018[69] and now constitutes the principal instrument of dual-use technology export control, affecting US-first exporters and foreign re-exporters alike (as well as some participants in US domestic commerce). Therefore, this regulation can be applied extraterritorially. The 2018 iteration of the export control rules constitutes the implementation of a strict, unified regime for the administration of the exports of dual-use technologies (in the civilian–military dichotomy), which follows a wave of moderate deregulation after the end of the Cold War to prevent hindering US exports and as a means of increasing American competitivity with other economies.

Today, the EAR mainly regulates the export of dual-use knowledge, items, and technologies subject to export controls specific to civilian (or at least non-military) implementations, constituting the cornerstone of the Dual-Use System for export control.[70] The scope of the Dual-Use System extends to 'commodities, software, or technologies that have both civilian and military applications'.[71] The system was administered under the Export Control Reform Act of 2018 (ECRA),[72] which ultimately imposes export restrictions on dual-use technologies within the powers of the executive branch, and more specifically, the president of the United States.[73] Determining which dual-use technology exports will be subjected to export controls, however, mainly falls under the jurisdiction of the BIS.

The scope of the US export control rules is established by enumerating the technologies to which they refer (without defining any form of dual use). As novel provisions of ECRA, when compared to the previous regime, and in response to

65 Weinberger, 2009, p. 156. The author points out that deemed exports are vaguely and generically defined, a conclusion valid even in light of the current regulatory regime. See: *Deemed exports*, no date.

66 *The International Traffic in Arms Regulation (ITAR)*, 2024.

67 *Export Authorization Regulations (EAR)*, 2024.

68 See: Alavi and Khamichonak, 2017, p. 67; Lazarou and Lokker, 2019, pp. 2–3.

69 Whang, 2021, pp. 19–20.

70 See: Congressional Research Service, 2020, pp. 2–4.

71 Congressional Research Service, 2020, p. 1.

72 *Export Control Reform Act of 2018*, 2018, secs. 2, 115.

73 For a description of the current provisions of the Export Control Reform Act of 2018, see: Congressional Research Service, 2021.

the growing (but by no means recent[74]) unease about geopolitical and geoeconomic rivalry with the PRC,[75] the act contains separate measures for emerging and foundational technologies (also named in the act as emerging critical technologies), by creating an interagency process under the supervision of the president of the US, to identify and regulate the export of such technologies. These technologies, pursuant to the ECRA, may be added to the Commerce Control List (sometimes also referred to as the BIS list), a solution that was previously applicable to less sensitive dual-use technologies.

While the act in force does not specifically enumerate the technologies to which this enhanced regime applies, according to the BIS, these should include technologies such as[76] additive manufacturing (popularly known as 3D printing), advanced computing technology, advanced materials (including nanomaterials), advanced surveillance technology, artificial intelligence and machine learning-related technologies, various biotechnologies, brain-computer interfaces, data analytics technologies, hypersonic technologies, (advanced) logistics technologies, microprocessor technology, position, navigation, and timing technologies (e.g. global positioning systems), quantum information and sensing technologies, and robotics.[77] Along with the possibility for the BIS to compile lists of proscribed items, the ECRA provides for administrative licencing of potentially dual-use exports (but also of foreign direct investment in situations where it might provide access to such technologies – a solution that blurs the lines between export controls and investment screening). During the licencing process, the presence of foreign entities or persons who would be considered a threat to US national security is also examined, and considered along with risks presented by the export to the US defence industrial base either in the form of a penury of the exported item, or based on broader economic concerns, such as a reduction in the US domestic production of items, the development of which was funded by federal resources, or the reduction of employment of persons with skills critical to national security within the US.[78] Due to the relative inability of the World

74 The US has been hostile to what it perceives as the "rise" of China and Chinese technological development for decades, citing reasons of economic competition, perceived as significant from the national security and technological superiority perspectives, demonstrating the securitisation of economic competition. See: McCormick, 2006; *Officials Show Scant Interest in Major Export Control Overhaul for China*, 2011.

75 Whang, 2021, p. 26; Gehrke and Ringhof, 2023b.

76 Congressional Research Service, 2021, p. 20; Tongele, 2022a, 2022b. A much wider list of technologies was considered as subsets of the ones listed above. See: Industry and Security Bureau, 2018.

77 Other technologies were added to this list, resulting from the 2019 update of the Wassenaar Arrangement, these being: 'hybrid additive manufacturing (AM) / computer numerically controlled (CNC) tools; computational lithography software designed for the fabrication of extreme ultraviolet (EUV) masks; technology for finishing wafers for 5nm production; digital forensics tools that circumvent authentication or authorisation controls on a computer (or communications device) and extract raw data; software for monitoring and analysis of communications and metadata acquired from a telecommunications service provider via a handover interface; and sub-orbital craft.' Congressional Research Service, 2021, p. 21.

78 Congressional Research Service, 2021, p. 24.

Trade Organization's (WTO's) General Agreement on Tariffs and Trade (GATT[79]) system to combat de-globalisation through the securitisation of world trade,[80] this system allows for provisions (Art. XXI(b)(ii) of the GATT in the 1994 version of the text) that permit the restriction of trade in case of shortages and for the defence of national security virtually without restriction, enabling the US to pursue a wide-ranging geoeconomic programme using export restrictions.

Therefore, the extant US export control regime, and specifically its new post-2018 provisions under the ECRA, aims for more than controlling dual-use technology outflows to protect national security imperatives. In fact, the regime instituted reflects what can be considered as a new, wider notion of economic security, or, more precisely the 'securitization of economic policy',[81] an attempt to maintain and enhance technological and economic advantages over not just adversaries such as the PRC,[82] but also simple competitors.[83]

The US export control regime also doubles as a de facto sanction regime, as the BIS maintains an Entity List,[84] which, unlike the proscribed technology lists, and specifically the control lists of the Wassenaar Arrangement referred to above, does not regulate dual-use knowledge, technology, or items in particular, but the entities to which exports of such items are effectively banned or subject to special conditions. This list contains numerous legal and natural persons, not just from states subject to sanctions but also from EU member states, thereby effectively hindering trade with the EU (albeit within the remit of US economic relations with EU member states).

The US unilateral export control regime effectively operates as an offensive geoeconomic tool[85] (not just as a simple sanction regime or embargo) because of the extraterritorial application of its rules: products that are manufactured outside the US but with export-restricted technology remain subject to it even if the products themselves do not incorporate restricted technology. In this manner, the US may leverage, and is known to have leveraged,[86] its technological might to interfere in commerce between third parties.

79 The name is the abbreviation of the General Agreement on Tariffs and Trade, 1947.

80 Bown, 2023.

81 Bown, 2020, pp. 287–289; Hrynkiv, 2022. The cited author sees the reasons for this securitisation in the transformative effects of digitalisation, and especially artificial intelligence, which increases competition between nations, and threatens to disrupt previous global economic and power hierarchies. In this context, export controls aim not only to defend national security, but also have a broader economic and technological supremacy over perceived adversaries, constituting a manifestation of deglobalisation, when coupled with other, apparently purely economic measures (such as politically, rather than economically motivated tariffs).

82 Bown, 2020, pp. 289–292.

83 Pillar, 2023.

84 For the current entity list, see: *Supplement No. 4 to Part 744, Title 15. Entity List*, 2024.

85 Bauerle-Danzman and Meunier, 2024, pp. 9–13.

86 See: Fägersten et al., 2023.

From these norms, it may be discerned, as has been duly observed,[87] that for geoeconomic reasons, the US desires to decouple from the PRC and acts to preserve and increase American advantages in the high-tech sector (currently specifically semiconductors), with possible adverse effects on the trade position of the EU and its member states.[88] Specifically, unlike the EU, the US utilises its export control regime in a punitive manner to impose specific sanctions on adversaries such as the PRC, while the EU adopts a country-neutral regime combined with specific sanctions to control the export of dual-use technology to states such as Russia.[89]

3.3. The EU dual-use regulation

The EU operates an export control regime comparable in complexity to that of the United States, which is meant to hinder the export of dual-use technologies, to enforce the international obligations of the member states pursuant to non-proliferation instruments adopted under the aegis of the United Nations (such as the Nuclear Non-Proliferation Treaty, the Chemical Weapons Convention, the Biological Weapons Convention, and UN Security Council Resolution 1540), to comply with international soft-law instruments that set up multilateral export control regimes, and to implement EU foreign policy measures, including various sanctions.[90] This regime is underpinned by the recently recast comprehensive Regulation (EU) 2021/821[91] (EUDUR). The EU dual-use technology regime may well be considered as a multilateral instrument, as, while the EU does have a legal personality under international law, its regulatory powers extend to member states.

Regulation (EU) 2021/821, as the previous applicable norm, does not stop member states from adopting dual-use technology export controls of their own, insofar as they do not contradict the provisions of the EU norm, a behaviour that has resulted in undue complications in determining applicable norms, and the risk of a "patchwork" legal regime.[92] According to the EUDUR, member states are beholden to enforce all international sanctions obligations, arising from '(…) sanctions imposed by a decision or a common position adopted by the Council or by a decision of the OSCE or by a binding resolution of the Security Council of the United Nations' (Article 15(1)(b), see also Recital no. (19)).

87 Gehrke and Ringhof, 2023a, 2023b; Fägersten et al., 2023, pp. 6–7.
88 Fägersten et al., 2023, pp. 55 et seq.; Chorzempa and von Daniels, 2023.
89 Gehrke and Ringhof, 2023b.
90 See: European Commission, 2024a.
91 *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*, 2021.
92 European Commission, 2024b, p. 8. To document national export controls for dual-use technology, the European Commission on 20 October 2023 published a list of national export controls. See: European Commission, 2023.

The specific solution for dual-use technology export control adopted by the EU is tailored to the structure of the EU itself, and therefore serves as a harmonisation instrument. The EUDUR creates a set of common rules for exports, including technical assistance and transit of items subject to export restrictions, of dual-use technology, as well as common criteria based on which the exports are to be assessed and authorisations are to be granted, common end-use controls, and catch-all rules for non-listed items (e.g. that may be used to restrict human rights in the course of cyber surveillance, or the manufacture of WMDs).[93] This part human rights-based approach, especially regarding the catch-all clause governing the export of technologies prone to use in cyber surveillance (to which I shall refer below during the discussion of dual-use AI), constitutes a specific aspect of the EU export control regime and one that was not universally accepted at the outset, in part because it placed the onus of vetting potential export destinations on the exporting entity, usually a private company.[94]

The EUDUR is the result of a recent trend in the EU, dictated by the European Commission, which has the aim of mobilising the bloc towards proactive participation in geoeconomic rivalries. in the post-2017 context of US–PRC tensions, tendencies for disengagement from multilateral organisations by the US, an increase in economic protectionism, and risks such as the Covid-19 pandemic and the flareup of the Russo–Ukraine war. In short, the regulation stems from the EU's intention to follow suit in the increasing securitisation of economic relationships by creating offensive and defensive geoeconomic tools, among which export controls occupy a significant position.[95]

This, especially with regard to the PRC, is in stark contrast to the pre-2017 period, during which, in the lack of any major security interest in the Asia-Pacific region, the EU placed emphasis on Eastward-bound trade and cooperation, while observing existing export restrictions, such as the arms embargo instituted against the PRC after 1989.[96]

This period ended in a series of near-collisions between EU and US policies towards the PRC, in which the US demonstrated a high degree of commitment towards securitising trade relations, and as part of a wider pressure campaign to force US allies to choose sides in the Indo-Pacific region's disputes, strong-arming the EU into adopting policies contrary to the initial intentions of the bloc, such as discouraging several EU member states from participating in the Asian Infrastructure Investment Bank or the Belt and Road Initiative.[97]

This demonstrates that centripetal forces in action between the US and the PRC are pushing the EU towards adopting measures, including in the domain of export

93 See: European Commission, 2024a.
94 Kanetake, 2019, pp. 159–161.
95 Bauerle-Danzman and Meunier, 2024, p. 13.
96 Bräuner, 2013, pp. 460–461.
97 Deng, 2020, pp. 113–118.

regulation, that now run counter to initial attempts at establishing interconnectivity and rare dictated by developments in a region that the EU, for a long time, prior to US-driven securitisation of economic relations – considered as one outside its sphere of strategic interest, as merely a partner and economic competitor, but not a security threat.[98]

The EU export control regime may be considered as long-suffering from various maladies that the recast version of the EUDUR (as well as previous iterations of its rules) has only partly addressed, such as difficulties in the mutual recognition of export licence documentation, the problems of firms established in several member states in correlating and adhering to the various national regimes, along with the common EU regime, and the information flow regarding end users of the exported technology, which is crucial for operating the catch-all rules of the regulation.[99] Some of these difficulties were partly addressed;[100] however, the current state of the regulation has not been immune to criticism (especially when it comes to transparency and the possibility of member states "taking over" measures adopted by other member states, a particularly pernicious problem if a common defence market is to be achieved). This criticism was levelled against several aspects of the EUDUR as follows:

1. The regulation continues to be a patchwork system, with a wide range of possibilities for member states to institute their own controls, parallel to the EU framework, a problem that is compounded by the fact that that these frameworks, in spite of the publication of a compilation of national rules in late 2023, lack transparency and are developed without sufficient consultation.
2. If member states decide to adopt (take over, as a measure permitted by the regulation) and implement controls previously enforced by other member states, there is little communication about when and how this may occur, a problem that particularly impacts catch-all measures specific to unilateral sanctions, which should be (but are not being) efficiently disseminated between the exporters of the various member states.
3. Member states may be barred by domestic rules from adopting export controls from other member states.
4. Forum shopping may occur when products cannot be directly exported from a given member state to a third country, but after transfer to another member state with more lenient rules for dual-use technology export, such an export may commence.
5. The lack of a common set of overall objectives in the field of export control policy, as member states hold the initiative in defining the contents of what is basically a multilateral regime (a problem that the White Paper on Export

98 Bauerle-Danzman and Meunier, 2024, p. 7.
99 *Chopping the Red Tape*, 1998, pp. 4–5.
100 *United States: Proposed Changes to the EU Dual-Use Export Control Regime*, 2016.

Controls proposes should be solved by extracting this domain from the ordinary legislative procedure).

6. The lack of common EU action internationally, as part of the EU common foreign and security policy, which also exposes some member states to strong-arming, even from partners.[101]

Thus, the EUDUR is an imperfect instrument that should be updated, keeping in mind the creation of a common set of EU-administered export rules, constituting a unified regime that may also benefit the common defence market currently taking shape.

3.4. The PRC's export control regime

Chinese policy on the development of civilian–military dual-use technology has shown significant novelty in recent years. Both direct and indirect instruments adopted in this area have increased in number and significance, starting in 2001, with a noticeable wave of regulation from 2015 to 2020. It demonstrates a policy trajectory towards enhanced bi-directional (military-to-civilian sector and civilian-to-military sector) technology transfer, as well as technological integration between military and civilian applications, including by breaking down confidence barriers between the military and civilian sectors, and by establishing common standards.[102]

This change in stance can be attributed to the broader set of policies enacted to achieve a wider economic transformation, by relying on emerging and transformative (digital) technologies as the drivers of future economic growth. The overall objective is avoiding the "middle income trap" that threatens the current structure of the PRC's economy.[103] Therefore, the PRC's efforts to attain a leading position in emerging and transformative technologies constitute more than a simple drive for modernisation, of which there have been many in the nation's history; they are driven by an imperative set in the strategic context of geopolitical rivalry. This perception stems from an expectation on behalf of PRC policymakers towards interference by the USA and other Western powers directed at the economic containment of the PRC,[104] which has, from the Chinese perspective, been partly realised by concrete measures, particularly those enacted by the US, directed against the export of technologies vital to the PRC's aspirations.

In response to measures undertaken by the US in the context of what is perceived on both sides of the Pacific as a wider geopolitical and geoeconomic rivalry (inter alia, by targeting PRC-registered companies for mixed, partly politicised reasons),

101 European Commission, 2024b, pp. 8–12.
102 Meng and Wang, 2023.
103 Qi and Chu, 2022, pp. 19–23.
104 Qi and Chu, 2022, p. 16.

the PRC has also enacted its first Export Control Law[105] (known as the ECL, replacing under this respect the less detailed provisions of the Foreign Trade Law), which came into force in 2020. Dual-use items are specifically mentioned as within the scope of this law, as well as a catch-all category comprising 'technologies, services and items relating to the maintenance of national security and national interests' (which constitute a novel element of the rule as opposed to the previous governance regime).[106] The ECL places the onus of identifying dual-use knowledge, items, or technologies subject to export control on the exporter. While the PRC's government does provide some lists of proscribed items, due to the lax formulation of the provisions of the law, its material scope may even be arbitrarily extended to other knowledge, items, or technology during the applicable administrative procedure when exporters apply for a licence.[107] During this procedure, the effects of granting the licence must also be examined, inter alia on considerations of national security and national interest, as well as on the "sensitivity" of the exported item itself.[108]

The export control regime instituted in the case of dual-use technologies by the PRC, dominated by the state in its administrative capacity, lends wider leeway to abuse than the previously examined systems, as the exporter is left to establish compliance mainly by its own devices, but it should be noted for its ability to rapidly adapt to changing technological realities.

4. Control regimes of some emerging dual-use technologies

The wide range of foundational, emerging, and disruptive dual-use technologies mentioned above require regulation to prevent major, even existential risks, not only to national but also global security, and to achieve non-proliferation. Therefore, not all such technologies may constitute the object of our analysis, and subjective selection is inevitably required.

This selection, while subjective, should at least partly consider the impact of the given disruptive dual-use technologies in the present and near future. Based on this criterion, in the following, I shall assess the specific regimes applicable to artificial intelligence, adjacent electronic processing (semiconductor technology), biotechnology, and 5G, leaving some other technologies, which I believe shall also have a serious impact later, to be analysed at another future occasion.

105 The State Council of China, 2021.
106 Köstner and Nonn, 2023, pp. 82–83, 87. The similarity with the US dual-use export regime should be noted here.
107 Köstner and Nonn, 2023, p. 92.
108 Köstner and Nonn, 2023, p. 92.

4.1. Artificial intelligence, advanced semi-conductor technology and quantum computing

Artificial intelligence (AI), considered one of the most important dual-use technologies under development, with a potentially transformative effect on most aspects of human existence, not only in the domain of information technology, but also in biotechnology and even warfare using dynamic weapons, constitutes one of the most significant objects of dual-use technology regulation, which is increasing in depth and volume.[109]

Several use-cases of AI being quite similar if not entirely identical in civilian and military applications (e.g. a self-driving "car" may very well be, in fact, also an armoured vehicle), the percolation of civilian AI development into the military field, along with robust research and development for exclusively military applications are a foregone conclusion. Considering the possibility of such diffusion, although some studies have shown that it is not (yet) very significant,[110] it is reasonable to assume that AI should constitute a major object of regulation meant to impede the free flow of technologies, specific items (e.g. microprocessors), and specialised knowledge.

In the case of AI, concerns of civilian technological advances being used for military purposes (according to the common dichotomy used to define dual use, especially from the European perspective) have been accompanied by concerns that some states (such as Russia or the PRC) or other non-state actors may view this technology through a different ethical prism, with less emphasis on basic human rights and freedoms, which may in turn facilitate utilising AI as a new, and from their perspective, very useful tool for social control. In this context, the expected utilisation of AI, although not a "classic" case of dual use, as the implementation nominally remains in the civilian (e.g. law enforcement) sphere, may also prove problematic and even threatening.[111]

It should be noted here that while dual-use technology regulation is nothing new, the regulation of AI-related items in the form of export controls, most definitely, is, as part of a renewed push, primarily by the US, to maintain its technological superiority over perceived adversaries,[112] a policy change that became more visible after the 2018 reform of US export regulations, as discussed above.

The restrictions on AI are by no means prompted exclusively based on trade and economic securitisation, or even human rights considerations, as the need for a new form of arms control is becoming more acute,[113] with cyberspace now considered a new and utterly different battlefield. While multilateral arms control

109 See: Ambrus, 2020; Top 10 Emerging Technologies Steering Group, 2023.
110 See: Schmid, Riebe and Reuter, 2022.
111 Schmid, Riebe and Reuter, 2022, pp. 2–3.
112 See: Shagina, 2023.
113 See: Dumbacher, 2018.

may be a modality by which AI, as an emerging technology, may be kept in check in the future, other means, such as export controls, are already being deployed in an attempt to manage risks, including misuse of AI to infringe on human rights, and also 'global security risks if democratic nations lose their current lead in AI'.[114] Assertions such as this make it clear that the ideological argument for technology control in the case of AI rests on a heterogeneous basis, including the maintenance of one trade bloc's advantage over others, or, as seen from Europe,[115] the maintenance of US advantage over all, even at the cost of subverting the global free trade system and the WTO (GATT) regime that was once at its core.

The regulation of dual-use AI technology is inconceivable without regulation of the processing equipment required to attain and operate it, which is why numerous measures for controlling advanced semiconductor exports and proliferation are practically aimed at technologies upon which AI implementations are based. Several export control targets must be considered for AI. These include general AI software, untrained algorithms and open-source datasets, specific AI software, trained algorithms and sensitive datasets, AI chip manufacturing equipment, and manufactured AI chips.[116]

Establishing a regulatory regime for AI has been the object of a major effort by the EU.[117] Finally, in a momentous act of legislative prowess, the EU AI Act (in fact a regulation according to the structure of EU instruments) was adopted.[118] It is noteworthy that while most risks of the use and abuse of AI were considered during the preparation of the AI Act, the problems of dual-use and export restrictions were not regulated. This may be explained by the scope of the instrument: the AI Act was specifically not meant to apply to military activities or the domain of national security (Recital (12a) and Article 2(3) of the Final Draft). While the act itself is intended to enforce human rights protection objectives, the notion of human rights is mostly omitted (except for the Recital (60m) of the final draft regarding artificial general intelligence).

This is not so in the US, where, partially as a reaction to the adoption of the AI Act, an Executive Order[119] was issued that explicitly refers to dual-use foundation models and their regulation (including exports and proliferation). Foundation

114 Flynn, 2020, p. 2.
115 Herrmann, 2023, pp. 2–4; Bauerle-Danzman and Meunier, 2024, p. 13.
116 Flynn, 2020, pp. 6–9.
117 For the most significant preparatory materials, see: Independent High-Level Expert Group on Artificial Intelligence, 2019a, 2019b, 2020b, 2020a.
118 The text of the Act has not been published in the Official Journal of the EU at the time that the manuscript of the present chapter was finalised. For the final draft, see: European Commission, Directorate-General for Communications Networks, Content and Technology, 2024.
119 The White House, 2023.

models constitute the essence[120] of generative AI, allowing "trained" algorithms to be applied to real-world situations, resulting in AI-generated feedback. This notion is also absent from the EU AI Act.

The EUDUR (with its content inspired by the Wassenaar Agreement regime) does not consider or regulate exports in the form of trained or untrained broad-purpose AI algorithms (such as machine learning or other algorithms implemented on hardware capable of operating neural networks), whereas it regulates specific algorithms for other uses in several situations (including cryptography and equipment operation). The regulation does govern exports of hardware that may be used for AI purposes (under items such as '3A001 – Electronic items', or '4A004 – Computers as follows and specially designed related equipment, "electronic assemblies" and components therefore').[121]

The EUDUR also implicitly governs the export of AI technologies (which in this case do include trained algorithms), through the interoperation of Article 2(1) (the definition of dual-use items, which includes software), Article 2(20) (which separately defines "cyber-surveillance items" as 'dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems') and the catch-all clause at Article 5(1), which requires authorisation for cyber-surveillance items not specifically listed,

> if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.[122]

120 A very recent definition of foundation models establishes the meaning of the term as follows: 'Foundation models constitute large-scale AI models that are pre-trained on vast amounts of general data and that can be adapted for downstream applications (e.g., by fine-tuning them through further training on application-specific data). Through this pre-train and adapt approach they expedite the development of innovative AI products and services and accelerate the accessibility of high-performance AI solutions in various industries (…). Foundation models show remarkable abilities to comprehend, generate, and adapt content across diverse domains, including creative generations (…), software debugging (…), protein sequencing (…), or cross-modality outputs such as text-to-image creations (…). With scaling, foundation models are becoming increasingly good at performing tasks they were not explicitly trained for, thereby broadening the scope of applications achievable by a single model without the need for additional training data or fine-tuning (…). When needed, task-specific performance can be further enhanced through fine-tuning or effective prompt engineering techniques; both of which incur significantly lower costs in comparison to developing a new model from scratch (…)'. Schneider, Meske and Kuss, 2024, p. 221.

121 The technical note of the EUDUR at item 4A004 reads as follows: 'For the purposes of 4A004.b., "neural computers" are computational devices designed or modified to mimic the behaviour of a neuron or a collection of neurons, i.e., computational devices which are distinguished by their hardware capability to modulate the weights and numbers of the interconnections of a multiplicity of computational components based on previous data.'

122 See: Vandenberghe, 2021.

In an approach that sets US regulations only slightly apart from the European model, the BIS specifically establishes restrictions on disruptive technologies, which include AI, with a view to strategic competition with the PRC (even if such restrictions are again centred mostly on hardware components and specifically microchips, that is, semiconductors, of a given ability),[123] a solution present in the EUDUR.

Such restrictions have been recently updated to include several new export control items:

> (…) 3A090, which concerns some advanced ICs that can have transfer rates of 600 gigabytes or more, (…) 3B090, which concerns semiconductor manufacturing equipment and related items, (…) 4A090, which concerns computers, assemblies, and components that include integrated circuits (ICs) over the limit delineated in 3A090a (…) 4D090, which concerns software tailored to developing items controlled under 4A090.[124]

Manufacturing equipment[125] for such advanced semiconductors is also the target of export restrictions.

These restrictions are dispersed and the Commerce Control (BIS) Lists,[126] true to the Wassenaar Arrangement model, only refer to processing equipment and encryption algorithms. The above-mentioned Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence covers algorithms but does not yet specifically regulate the export of general-purpose AI algorithms.

This approach (prevalent in the literature between 2017 and 2020) is accredited in theory by considering that general-purpose AI algorithms would be harder to regulate, and the choke-point that should be targeted by dual-use technology export regulations, is primarily the semiconductor industry.[127] However, this method of regulation tends to ignore recent and dramatic advances in generative AI (such as ChatGPT), which, although having a general purpose, shows impressive potential as a direction for technological development.

The focus on advanced semiconductors and computer assemblies (as well as only some specialised algorithms) by the EU and US regulators alike, with the EU rules enhanced by human rights protection clauses, begs the question of whether a catch-all clause would have to be included in the norms, to extend the rules to general-purpose AI algorithms, as well as some commonly recognised threat actors, to permit cooperation and create an environment in which free trade and security concerns may coexist, as much as possible.

123 Bureau of Industry and Security, 2022, 2023a.
124 Reinsch, Schleich and Denamiel, 2023.
125 Bureau of Industry and Security, 2023a; *The United States Announces Export Controls to Restrict China's Ability to Purchase and Manufacture High-End Chips*, 2023.
126 See: Bureau of Industry and Security, 2024a, 2024b, 2024c.
127 Flynn, 2020.

Another potential problem is the use of AI in cyberweapons, such AI algorithms could be subject to rules on military technology exports[128] if they are clearly incorporated into such technology, but otherwise, and unless their purpose is clearly military, they may escape regulation altogether.

With major export control efforts directed at containing the proliferation of advanced semiconductor technology, another aspect is overlooked and perhaps more difficult to control by either the US or EU export control regimes. Human resource migration towards states (particularly the PRC), which are the subject of clearly stated or thinly veiled measures aiming to control the flow of certain dual-use technologies, is difficult to subject to similar "export" controls as hardware components and manufacturing technologies.[129] Without considering the flow of human resources, dual-use technology regulation as a singular measure may be necessary but by no means sufficient for the stated aims of containing the complex set of technologies that result in AI applications, even if the notion of "export" is usually defined to include revealing sensitive information (as in the case of deemed exports).

A specific field adjacent to AI, which should be mentioned owing to its potentially transformative nature and significant dual-use potential, is quantum computing. While not a discipline strictly linked to AI, quantum computing may result in revolutionising different aspects of information technology in the fields of encryption and communication, rendering most modern techniques of encryption useless, and permitting forms of communications that through a phenomenon known as quantum entanglement results in instant, tamper-proof communications, possibly over incredible distances; quantum metrology also presents significant dual-use potential as developments in this field may lead to highly enhanced location sensors.[130]

While the Wassenaar Arrangement regime, and thus the EU and US export control regimes,[131] also envisage some software applications that would either be implemented on quantum computing systems or would be immune to the impact of such systems on traditional means of electronic encryption, neither of these regimes currently refers to specific quantum computing hardware, as the technical characteristics of such hardware would be difficult to grasp and discern at this moment. Therefore, as stated in the literature and in a manner somewhat similar to the case of disruptive biotechnologies discussed below, soft-law methods of governance, such as codes of conduct and voluntary compliance programmes, are possible methods for preventing the proliferation of dual-use quantum computing.[132]

128 Herr and Rosenzweig, 2016.
129 Chu, 2008.
130 Johnson, 2019.
131 E.g. At item 5A002. *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*, 2021; Bureau of Industry and Security, 2024b.
132 Johnson, 2019.

4.2. Biotechnology

Biotechnology (and its various subfields, such as genetics, genomics, biochemistry, virology, bacteriology, and biology-related nanotechnology) is a complex subject of regulation. Entry limits in the biotechnological domain are far removed from the difficulties posed by past disruptive technologies, such as nuclear weapons systems (although such impediments are still more consistent than those for information technology). In fact, with increased globalisation of both knowledge and technological means to affect biological and biochemical research (in this field, often referred to as dual-use research of concern, abbreviated as DURC), a completely new set of absurdly dangerous dual-use scenarios has emerged. These include the laboratory synthesis or enhancement of dangerous pathogens, such as the machine-based generation of the 1918 influenza virus, of various poxviruses, or artificially increasing the transmissibility of the H5N1 zoonotic influenza virus between mammals, or AI-aided discoveries for the manufacturing of known (and possibly unknown) toxins, such as the VX nerve agent.[133] The advent of CRISPR/Cas9 as a method of reasonably accurate gene editing has added an entirely new layer of risk, as it makes large-scale interventions into the DNA and RNA of existing organisms practically feasible, with the added risk that the proliferation of this technology is not easily controlled.[134] A third layer of complexity is added by combining the above technologies with AI, resulting in machine-learned methods for generating toxins, or enhancing pathogens (gain of function experiments); such combinations render much if not most of the research that makes use of technological synergies, dual-use.[135] These examples underline the interconnectedness of some dual-use technologies, as information technology is integral to modern biotechnological research, with the dangerous prospects of synthetic biology (the possibility of creating or enhancing living organisms, or even new types of organisms that do not exist yet) vastly increasing the risks of unintended consequences, including dual-use scenarios.[136]

Development critical to advancements in medicine and pharmacology usually occurs in the private sector; therefore, voluntary compliance with the regimes imposed for dual-use technology regulation is paramount. However, no such centralised regime is forthcoming; a problem specific to the dual-use dilemma in life sciences seems to be the heightened significance of ethics rules and bodies, along with the lack of a workable definition for dual use[137] (which seems to plague life sciences as much as legal science). The very notion of dual use has gained an entirely new meaning in the field of biotechnology, one which is different from those

133 Urbina et al., 2022.
134 See: Mir et al., 2022.
135 Evans, 2022.
136 For the dilemma posed by publishing the methodology of an experiment aimed at synthetically enhancing the H5N1 strain of influenza, see: Rager-Zisman, 2012.
137 Dubov, 2014.

utilised in the "classical" instruments for governing dual-use technologies.[138] In this domain, "dual use" is not only employed to refer to potential military applications, or even just nefarious applications of a given technology, but also to unethical (e.g. unintended) use in general.[139] Therefore, legal dual-use regimes are doubled in life sciences by science ethics supervision,[140] adding a list of government and academic supervisory bodies (including editorial and ethics boards organised outside clearly defined legal frameworks) and authorities to the regulatory mix, with competences not only regarding the international or domestic (deemed) export of such technologies but also a myriad of other competences and activities.[141]

The promotion of self-regulation in this domain is therefore necessary, at least to complement extant and future sources of law. This solution is also justified by the high rate of voluntary compliance with such regimes, as well as the ability of the private sector to institute consortia that would impose compliance with the standards set, with sufficient assistance from government. This is so, first, to contain non-compliant industry actors and encourage them to join self-regulating bodies and abide by their common rules and practices, and second, to dispel industry secrecy, which would be counter-productive for enforcement.[142]

A multi-tiered approach has recently been proposed for managing the risks posed by dual-use technology development, which is specifically suitable for biotechnology and may be deployed in the stages of early development by scientific institutions, functioning in conjunction with domestic and international normative regimes. According to this approach, self-governing bodies, research funding agencies, regulators, and publishers should all consider the risks posed by the given technology for dual use (including nefarious use), properly screen the personnel researching and operating the technology, share data regarding the participants in dual-use research, consider the results of dialogue with civil society in general when developing directions of research, weigh the need for research with inherent risks to determine future risks and enhance governance, and finally adapt scientific publication practices (including publication in preprints) to prevent undesired knowledge or technologies from being published.[143] As a manifestation of this approach, the World Health Organization, beginning in the early 2010s, examined (though ultimately rejected[144]) measures to suppress the publication of possibly dual-use knowledge regarding some pathogens.[145]

138 Campbell, 2006.
139 Pustovit and Williams, 2010; van der Bruggen, 2012, pp. 745–748.
140 Rychnovská, 2016.
141 A case in point is US academic biotechnology research supervision. See: Fox, 2004.
142 Maurer and Fischer, 2010.
143 Yoshizawa et al., 2023. This approach, as the authors show, would in turn limit the scope of open science. The problem of limiting open science in turn, particularly in life sciences and biotechnology, is treated partly as a philosophical question (see: Selgelid, 2009; 2013), in lack of regulatory input through hard-law instruments.
144 Rager-Zisman, 2012.
145 Stone, 2012.

In enforcing this multitiered approach, the definition of dual use is of paramount importance. One of the best proposed definitions (which only covers research) originates from the American National Research Council of the National Academies' Fink report,[146] which aggregates all definitions of dual use to which I have referred.[147] Thus, the purpose-definition problem of dual-use persists in biotechnology.

Regarding legislative (i.e. soft law, hard law, or black letter law) regimes governing dual use in the life sciences, the Biological Weapons Convention (as the Biological and Toxin Weapons Convention of 1972) did not initially envisage the dual-use problem, perhaps owing to the lower level of interconnectedness in the domain of biological research at the time of adoption. However, after the 11 September 2001 attacks and the associated acts of bioterrorism, this approach was reconsidered, and the Sixth Review Conference of the convention, in its 2006 Final Document,[148] did consider the factors of dual-use items (i.e. pathogens) and knowledge,[149] thereby implicitly recognising the possibility that the convention's regime may be extended to such situations.

The EUDUR, continuing the tradition of previous norms,[150] does not specifically refer to a dual-use regime in the field of biotechnology (the civilian–military dichotomy forms the basis of the regulation as discussed above). However, the EUDUR implements protective measures for some dual-use technologies specific to the field of biotechnology, after its most recent update,[151] such as subjecting to licencing the export of '"Software" specially designed for nucleic acid assemblers and synthesisers specified in 2B352.i., that is capable of designing and building functional genetic elements from digital sequence data' as per Annex I subcategory 2D352 of the EUDUR.[152]

Further, historically the EUDUR has restricted the export of laboratory equipment, which in turn may be of dual use (e.g. under subcategory '2B352 Biological manufacturing and handling equipment'). Some pathogens and substances with biotechnological relevance are also subject to the EUDUR, such as those under the Technical Notes for item 1C353 (e.g. biological agents that would reduce immune responses).[153]

In addition, in the context of European geoeconomic securitisation, significant member states have lowered the thresholds for investment screening (France and

146 Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, 2004; van der Bruggen, 2012, p. 754.
147 See: Selgelid, 2009, p. 176; van der Bruggen, 2012, p. 754.
148 *Final Document of the BWC Sixth Review Conference*, 2006.
149 van der Bruggen, 2012, pp. 743–744.
150 See: Czarkowski, 2010.
151 Raivo and Triščuka, 2023.
152 Subcategory 2B352.i. of the EUDUR refers to 'Nucleic acid assemblers and synthesisers, which are partly or entirely automated, and designed to generate continuous nucleic acids greater than 1,5 kilobases in length with error rates less than 5 % in a single run'.
153 Erbay, 2023, pp. 25–26.

Germany) and have even introduced intra-EU investment screening (Italy and Spain) in the biotechnology sector.[154]

The US BIS proscribed item lists also contain materials and agents that are relevant for the development of biotechnologies and the limited access knowledge required for such undertakings,[155] similar to the EUDUR.

4.3. 5G Communications

In the field of wideband communications, and regarding the technology generally known as 5G, the dual-use dilemma takes a new shape: export controls in this situation become secondary to foreign direct investment considerations, and import controls enacted as part of an effort by the US and its allies to stem the growing influence of the PRC in this sector.

Technological dominance in the field of 5G[156] as a potentially disruptive and transformative emerging technology, also given its possible synergies with other emerging technologies, such as AI, robotics and the "Internet of Things" is considered key in the securitisation of national economies. This field is currently dominated by the US (through domestic 5G chip supplier Qualcomm, and the collaboration between Taiwanese company MediaTek and US-based Intel), with Samsung (South Korea), and Huawei (a PRC-controlled, ostensibly independent company), the other participants in a 'very narrow playing field'.[157] As a manifestation of the push for securitisation of the telecommunications industry, the US and its allies have invoked various concerns, including the possibility of back doors built into 5G systems supplied by manufacturers based in the PRC, but also the unacceptable system of values gaining prominence along with Huawei's technological development, such as online censorship and a breakdown of the openness that should characterise the increasingly liberal global culture, in the name of "cyber-sovereignty".[158]

In the hostile climate generated by the US–PRC strategic competition, and against the backdrop of administrative measures by the US to exclude Huawei and other PRC-based companies from developing domestic 5G infrastructure, significant EU member states such as Germany have found themselves confronted with the dilemma of lining up behind what are essentially trade and investment policies

154 Bauerle-Danzman and Meunier, 2024.

155 See: Bureau of Industry and Security, 2023b; *Deemed Exports and Fundamental Research for Biological Items*, 2024.

156 Bartholomew, 2020.

157 Moore, 2023.

158 Bartholomew, 2020; Moore, 2023. Such concerns are by no means far-fetched as the PRC has taken a leading role in global policymaking when it comes to setting the operational standards of the Internet, and seems to have favoured the adoption of solutions and technical standards that permit a greater control over cyberspace, inter alia by favouring the introduction of state controlled points of access, and a reduction of the fabled anonymity that characterised the Internet's earlier phases of development, including by making the identification of real-world identities of Internet users easier. Yoo and Mueller, 2024.

dictated by US securitisation concerns or following previously laid plans for 5G infrastructure development.[159] Until recently, this dilemma has produced little in the way of a decisive break with Huawei as a leading 5G technology manufacturer; however, a reduction in reliance on this manufacturer's technology in critical infrastructure has been proposed and is being implemented[160] by means of import and investment controls (mostly left in the sphere of competence of EU member states). When it comes to compliance with US requests for exclusion, by legislative means, of Huawei from the development of 5G infrastructure, one recent study[161] has convincingly demonstrated that the positioning of secondary states, such as NATO and EU member states in the US–PRC rivalry is determined by the patron-client theory of international relations, with the most significant factor in rendering a policy response towards exclusion of PRC-based actors from 5G development being the security guarantees granted to a state by the US (this point being validated, including for EU member states).

This said, Germany, as one of the EU's leading economic powers, and a significant actor in EU-level regulation, in a way representative of the entire EU, has adopted a stance of cautious cooperation with US policies,[162] and other measures against the PRC in the field of emerging, and disruptive dual-use technologies, which is likely to determine the fate of 5G development in the future.

5. Conclusions

I have attempted to offer as comprehensive a view as possible, considering the medium used, pertaining to the topic of dual-use technology regulation and the regulatory regime applicable to some major emerging and disruptive dual-use technologies.

In a field dominated by mistrust and rivalry between technological powers, and a wide array of normative instruments, some of a binding nature, others constituting soft law, it may be stated that several considerations interact to create the fuzzy notion of "dual use": military and civilian use, and benign and nefarious use are at the poles of various dichotomies, leading to a combined risk-based approach that emphasises (presumed, or possible) intention. As such, the definitions of dual use in various instruments and regimes only partly overlap, leading to uncertainty as to whether, and more importantly, why, some elements of emerging and disruptive technologies should be considered dual-use, whereas others should not. This

159 Krolikowski and Hall, 2023.
160 Sarah, Andreas and Hakan, 2023.
161 Christie, Jakobsen and Jakobsen, 2024.
162 Cook, Ohle and Han, 2022.

situation is further complicated by the ethics-based approach to dual use prevalent in the fields of molecular biology and related biotechnology, which, in turn, interacts with applied information technology and AI.

The presumed and possible intentions of parties, as well as the geoeconomic interests of some actors in an atmosphere of securitisation of scientific research, trade, and techno-economic development, combine in various unilateral and bilateral instruments to result in governance regimes where considerations for restricting the flow of dual-use knowledge, items, and technologies no longer follow the previous track of avoiding military or nefarious use, while remaining permissive to global trade.

In this environment, the EU, through the EUDUR, an imperfect but useful instrument, has attempted to provide a principal, not just a geo-economic basis for considering the defence of fundamental human rights and freedoms, within a catch-all clause to prevent the misuse of information technology to achieve greater levels of surveillance. In turn, the US has sought to endow economic advantage and technological superiority with national security significance and has tailored its dual-use export regime to maintain this primacy as a manifestation of securitisation. The PRC has followed a similar track, while multilateral institutions and supra-regional instruments have been mostly ignored or sidelined, complicated by geopolitical realities, such as Russia's membership in the Wassenaar Arrangement.

I have shown that both in the field of artificial intelligence, and the related field of biotechnology, regulatory regimes, which do exist in the "classical" instruments of dual-use technology governance, must be complemented by voluntary compliance and ethical standards. Further, specifically in the field of AI, a lack of proper definitions of artificial intelligence, and governance of AI algorithms as dual-use technologies unto themselves is still present (although the "hardware" component of AI systems in the form of semiconductors is highly regulated).

Any future regulator of dual use, including the EU, has to walk a tightrope between overly permissive and overly restrictive norms, something that is problematic in the current environment of strengthening restrictions. Specifically human-rights based approaches, such as those used by the "European model" for restricting proliferation of disruptive, emerging dual-use technologies should be more widely considered as part of such efforts, to the detriment of economic securitisation.

References

Alavi, H., Khamichonak, T. (2017) 'EU and US Export Control Regimes for Dual Use Goods: An Overview of Existing Frameworks', *Romanian Journal of European Affairs*, 17(1), pp. 59–74.

Ambrus, É. (2020) 'Artificial Intelligence as a Dual-use Technology', *Academic and Applied Research in Military and Public Management Science*, 19(2), pp. 19–28; https://doi.org/10.32565/aarms.2020.2.2.

Arms Control Association (2022) 'The Wassenaar Arrangement at a Glance'. [Online]. Available at: https://www.armscontrol.org/factsheets/wassenaar (Accessed: 15 February 2024).

The Australia Group (no date a) *Objectives of the group*. [Online]. Available at: https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/objectives.html (Accessed: 15 November 2023).

The Australia Group Australia (no date b) *Guidelines for Transfers of Sensitive Chemical or Biological Items*. [Online]. Available at: https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/guidelines.html (Accessed: 10 October 2023).

Bartholomew, C. (2020) 'China and 5G', *Issues in Science and Technology*, 36(2), pp. 50–57.

Bauerle-Danzman, S., Meunier, S. (2024) 'The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator', *JCMS: Journal of Common Market Studies*, 62(4); https://doi.org/10.1111/jcms.13599.

Blanken, L.J., Lepore, J.J. (2024) 'Trade Policy for Dual-Use Technology', *Defence and Peace Economics*, 35(2), pp. 192–205; https://doi.org/10.1080/10242694.2022.2145645.

Bown, C.P. (2020) 'Export Controls: America's Other National Security Threat', *Duke Journal of Comparative & International Law*, 30(2), pp. 283–308, Available at: https://scholarship.law.duke.edu/djcil/vol30/iss2/4 (Accessed: 17 March 2024).

Bown, C.P. (2023) 'The Challenge of Export Controls', *Finance & Development*, 60(2), pp. 18–21.

Brandt, L. (1994) 'Defense Conversion and Dual-Use Technology', *Policy Studies Journal*, 22(2), pp. 359–370; https://doi.org/10.1111/j.1541-0072.1994.tb01474.x.

Bräuner, O. (2013) 'Beyond the Arms Embargo: EU Transfers of Defense and Dual-Use Technologies to China', *Journal of East Asian Studies*, 13(3), pp. 457–482; https://doi.org/10.1017/S1598240800008304.

Bremer-Maerli, M., Johnston, R.G. (2002) 'Safeguarding This and Verifying That: Fuzzy Concepts, Confusing Terminology, and Their Detrimental Effects on Nuclear Husbandry', *The Nonproliferation Review*, 9(1) pp. 54–82; https://doi.org/10.1080/10736700208436874.

van der Bruggen, K. (2012) 'Possibilities, Intentions and Threats: Dual Use in the Life Sciences Reconsidered', *Science and Engineering Ethics*, 18(4), pp. 741–56; https://doi.org/10.1007/s11948-011-9266-2.

Brunk, G.G., Jason, G.J. (1981) 'The impact of warfare on the rate of invention: A time series analysis of United States patent activity', *Scientometrics*, 3(6), pp. 437–455; https://doi.org/10.1007/BF02017436.

Bureau of Industry and Security (2022) 'Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)', 17 October. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3355-2023-10-17-bis-press-release-acs-and-sme-rules-final-js/file (Accessed: 15 December 2023).

Bureau of Industry and Security (2023a) 'Commerce Strengthens Restrictions on Advanced Computing Semiconductors, Semiconductor Manufacturing Equipment, and Supercomputing Items to Countries of Concern', 17 October. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3355-2023-10-17-bis-press-release-acs-and-sme-rules-final-js/file (Accessed: 15 December 2023).

Bureau of Industry and Security (2023b) 'Supplement No. 1 to Part 774, Title 15. Category 1', 8 December. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2332-category-1-materials-chemicals-microorganisms-and-toxins-4/file (Accessed: 30 January 2024).

Bureau of Industry and Security (2024a) 'Supplement No. 1 to Part 774, Title 15. Category 4', 13 March. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2335-ccl4-5/file (Accessed: 30 March 2024).

Bureau of Industry and Security (2024b) 'Supplement No. 1 to Part 774, Title 15. Category 5 Part 1', 17 November. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2337-ccl5-pt2-4/file (Accessed: 30 March 2024).

Bureau of Industry and Security (2024c) 'Supplement No. 1 to Part 774, Title 15. Category 5 Part 2', 13 March. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/regulations-docs/2336-ccl5-pt1-3/file (Accessed: 30 March 2024).

Buzan, B., Wæver, O. (2009) 'Macrosecuritisation and security constellations: reconsidering scale in securitisation theory', *Review of International Studies*, 35(2), pp. 253–276; https://doi.org/10.1017/S0260210509008511.

Bzhilianskaya, L.Y. (1996) 'Civil applications of dual-use technology in Russia' in Mitcham, C. et al. (eds.) *1996 International Symposium on Technology and Society: Technical Expertise and Public Decisions. Proceedings*. Princetown, New Jersey: IEEE, pp. 25–34; https://doi.org/10.1109/istas.1996.540423.

Campbell, P. (2006) 'Empowerment and restraint in scientific communication: New developments make it easier to share information, but more difficult to deal with dual-use biology', *EMBO Reports*, 7(SI), pp. S18–22; https://doi.org/10.1038/sj.embor.7400710.

Chemical Weapons Convention (1993) Paris, New York, NY, 13 January 1993. [Online]. Available at: https://www.opcw.org/chemical-weapons-convention (Accessed: 5 November 2023).

Chorzempa, M., von Daniels, L. (2023) 'New US Export Controls: Key Policy Choices for Europe', *SWP Comment*, 2023/C 20, 24 March 2023, *Stiftung Wissenschaft und Politik*; https://doi.org/10.18449/2023C20.

Christie, Ø.S., Jakobsen, J., Jakobsen, T.G. (2024) 'The US Way or Huawei? An Analysis of the Positioning of Secondary States in the US-China Rivalry', *Journal of Chinese Political Science*, 29(1), pp. 77–108; https://doi.org/10.1007/s11366-023-09858-y.

Chu, M.-C.M. (2008) 'Controlling the Uncontrollable: The Migration of the Taiwanese Semiconductor Industry to China and Its Security Ramifications', *China Perspectives*, 2008/1, pp. 54–68; https://doi.org/10.4000/chinaperspectives.3343.

Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology (2004*) Biotechnology Research in an Age of Terorism*. Washington, DC: The National Academies Press. [Online]. Available at: https://nap.nationalacademies.org/catalog/10827/biotechnology-research-in-an-age-of-terrorism (Accessed: 25 October 2023).

Congressional Research Service (2020) 'The U.S. Export Control System and the Export Control Reform Initiative' R41916, 28 January. [Online]. Available at: https://sgp.fas.org/crs/natsec/R41916.pdf (Accessed: 20 November 2023).

Congressional Research Service (2021) 'The U.S. Export Control System and the Export Control Reform Act of 2018' R46814, 7 June. [Online]. Available at: https://crsreports.congress.gov/product/pdf/R/R46814 (Accessed: 20 November 2023).

Cook, R.J., Ohle, M., Han, Z. (2022) 'The Illusion of the China-US-Europe Strategic Triangle: Reactions from Germany and the UK', *Journal of Chinese Political Science*, 27(3), pp. 493–518; https://doi.org/10.1007/s11366-021-09771-2.

Czarkowski, M. (2010) 'The Dilemma of Dual Use Biological Research: Polish Perspective', *Science and Engineering Ethics*, 16(1), pp. 99–110; https://doi.org/10.1007/s11948-008-9078-1.

Davis, I. (2002) *The Regulation of Arms and Dual-Use Exports. Germany, Sweden and the UK*. Oxford: SIPRI – Oxford University Press. Available at: https://www.sipri.org/sites/default/files/files/books/SIPRI02Davis.pdf (Accessed: 27 October 2023).

Deng, Y. (2020) 'The Role of the EU in Asian Security: Between Transatlantic Coordination and Strategic Autonomy', *Asia Policy*, 15(1), pp. 105–126; https://doi.org/10.1353/asp.2020.0001.

Dubov, A. (2014) 'The concept of governance in dual-use research', *Medicine, Health Care and Philosophy*, 17(3), pp. 447–457; https://doi.org/10.1007/s11019-013-9542-9.

Dumbacher, E.D. (2018) 'Limiting cyberwarfare: applying arms-control models to an emerging technology', *The Nonproliferation Review*, 25(3–4), pp. 203–222; https://doi.org/10.1080/10736700.2018.1515152.

Erbay, C. (2023) T*he Third Biotechnology Revolution: Synthetic Biology and its Regulation in the European Union*. Tilburg: Tilburg University. [Online]. Available at: https://arno.uvt.nl/show.cgi?fid=162927 (Accessed: 30 September 2023).

European Commission (2023) 'Compilation of national control lists under Article 9(4) of Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, PUB/2023/1267' OJ C C2023/441, 20 October. [Online]. Available at: https://eur-lex.europa.eu/eli/C/2023/441/oj (Accessed: 20 December 2023).

European Commission (2024a) *Exporting dual-use items*. [Online]. Available at: https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en (Accessed: 15 February 2024).

European Commission (2024b) 'White Paper on Export Controls' COM(2024) 25 final, 24 January. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0025 (Accessed: 1 March 2024).

European Commission, Directorate-General for Communications Networks, Content and Technology (2024) 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Analysis of the final compromise text with a view to agreement'. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf (Accessed: 25 February 2024).

Evans, S.W. (2022) 'When All Research Is Dual Use', *Issues in Science and Technology*, 38(3), pp. 84–87.

Export Authorization Regulations (EAR) (2024) *Bureau of Industry and Security*. [Online]. Available at: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear (Accessed: 19 February 2024).

Export Control Reform Act of 2018 (2018) U.S. Congress, 15 February 2018. [Online]. Available at: https://www.congress.gov/bill/115th-congress/house-bill/5040/text (Accessed: 19 September 2023).

Fägersten, B., Lovcalic, U., Regnér, A.L., Vashishtha, S. (2023) 'Controlling critical technology in an age of geoeconomics: Actors, tools, and scenarios', *The Swedish Institute of International Affairs*, 2023/1. [Online]. Available at: https://www.ui.se/globalassets/butiken/ui-report/2023/ui-report-no.1-2023.pdf (Accessed: 18 February 2024).

Floyd, R. (2007) 'Towards a consequentialist evaluation of security: bringing together the Copenhagen and the Welsh Schools of security studies', *Review of International Studies*, 33(2), pp. 327–350; https://doi.org/10.1017/S026021050700753X.

Flynn, C. (2020) 'Recommendations on Export Controls for Artificial Intelligence', *Center for Security and Emerging Technology Issue Brief*, February 2020. [Online]. Available at: https://cset.georgetown.edu/publication/recommendations-on-export-controls-for-artificial-intelligence/ (Accessed: 18 February 2024).

Forge, J. (2010) 'A Note on the Definition of "Dual Use"', *Science and Engineering Ethics*, 16(1), pp. 111–118; https://doi.org/10.1007/s11948-009-9159-9.

Fox, J.L. (2004) 'US to safeguard "dual-use" biology research', *Nature Biotechnology*, 369(22); https://doi.org/10.1038/nbt0404-369.

Fuhrmann, M. (2008) 'Exporting Mass Destruction? The Determinants of Dual-Use Trade', *Journal of Peace Research*, 45(5), pp. 633–652; https://doi.org/10.1177/0022343308094324.

Gearon, L. (2017) 'The counter-terrorist campus: Securitisation theory and university securitisation – Three Models', *Transformation in Higher Education*, 2(a13); https://doi.org/10.4102/the.v2i0.13.

Gearon, L., Parsons, S. (2019) 'Research Ethics in the Securitised University', *Journal of Academic Ethics*, 17(1), pp. 73–93; https://doi.org/10.1007/s10805-018-9317-2.

Gehrke, T., Ringhof, J. (2023a) 'Caught in the crossfire: Why EU states should discuss strategic export controls', *European Council on Foreign Relations* [Preprint], 11 January 2023. [Online]. Available at: https://ecfr.eu/article/caught-in-the-crossfire-why-eu-states-should-discuss-strategic-export-controls/ (Accessed: 24 November 2023).

Gehrke, T., Ringhof, J. (2023b) 'The power of control: How the EU can shape the new era of strategic export restrictions', *European Council on Foreign Relations*, 17 May 2023. [Online]. Available at: https://ecfr.eu/publication/the-power-of-control-how-the-eu-can-shape-the-new-era-of-strategic-export-restrictions/ (Accessed: 24 November 2023).

Gewirtz, P. (1996) 'On "I Know It When I See It"', *The Yale Law Journal*, 105(4), pp. 1023–1047; https://doi.org/10.2307/797245.

Grahame, D., Mendelsohn, J. (eds.) (2002) *Arms Control Chronology*. Washington, DC: The Center for Defense Information.

Griffiths, P. (2019) 'Updates from the Wassenaar Arrangement', *SMi FourteenthAnnual Conference Defence Exports*, pp. 1–8.

Herr, T., Rosenzweig, P. (2016) 'Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model', *Journal of National Security Law & Policy*, 8(2), pp. 301–319.

Herrmann, C. (2023) 'Open Strategic Autonomy – New challenges for the EU's Common Commercial Policy' *SIEPS – Swedish Institute for European Policy Studies*, June 2023. [Online]. Available at: https://www.sieps.se/globalassets/publikationer/2023/2023_9epa.pdf (Accessed: 9 September 2023).

Himmelfreundpointner, R. (2017) 'Le Monde Wassenaar Arrangement', *Cercle Diplomatique*, 2017/1, pp. 62–66.

Hofhansel, C. (1993) 'From containment of communism to Saddam: The evolution of export control regimes', *Arms Control*, 14(3), pp. 371–404; https://doi.org/10.1080/01440389308404046.

Hrynkiv, O. (2022) 'Export Controls and Securitization of Economic Policy: Comparative Analysis of the Practice of the United States, the European Union, China, and Russia', *Journal of World Trade*, 56(4), pp. 633–656; https://doi.org/10.54648/trad2022026.

Independent High-Level Expert Group on Artificial Intelligence (2019a) 'A Definition of AI: Main Capabilities and Disciplines' *Brussels: European Commission*, 8 April. [Online]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651 (Accessed: 5 April 2023).

Independent High-Level Expert Group on Artificial Intelligence (2019b) 'Ethics Guidelines for Trustworthy AI' *Brussels: European Commission*, 8 April. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Accessed: 5 April 2023).

Independent High-Level Expert Group on Artificial Intelligence (2020a) 'Assessment List for Trustworthy Artificial Intelligence' *Brussels: European Commission*, 17 July. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (Accessed: 5 April 2023).

Independent High-Level Expert Group on Artificial Intelligence (2020b) 'Sectoral Considerations on the Policy and Investment Recommendations for Trustworthy Artificial Intelligence' *Brussels: European Commission*. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (Accessed: 5 April 2023).

Industry and Security Bureau (2018) 'Review of Controls for Certain Emerging Technologies', 19 November. [Online]. Available at: https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies (Accessed: 15 November 2023).

Johnson, W.G. (2019) 'Governance Tools for the Second Quantum Revolution', *Jurimetrics*, 59(4), pp. 487–521.

Kanetake, M. (2019) 'The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches', *Business and Human Rights Journal*, 4(1), pp. 155–162; https://doi.org/10.1017/bhj.2018.18.

Katz, J.I. (2020) 'Education and Training as a Disruptive Dual Use Technology' in Martellini, M., Trapp, R. (eds.) *21st Century Prometheus: Managing CBRN Safety and Security Affected by Cutting-Edge Technologies*. 1st edn. Cham: Springer International Publishing, pp. 205–210; https://doi.org/10.1007/978-3-030-28285-1_10.

Kelsen, H. (1991) 'Legal Norms and Legal Principles: Esser's Transformation Theory' in Kelsen, H., Hartney, M. (eds.) *General Theory of Norms*. online edn. Oxford: Oxford Academic, pp. 115–122; https://doi.org/10.1093/acprof:oso/9780198252177.003.0028.

Kim, H. (2021) 'Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue', *The International and Comparative Law Quarterly*, 70(2), pp. 379–415; https://doi.org/10.1017/S0020589321000105.

Klaus, M.D. (2003) 'Dual-Use Free Trade Agreements: The Contemporary Alternative to High-Tech Export Controls', *Denver Journal of International Law & Policy*, 32(1), pp. 105–134.

Köstner, D., Nonn, M. (2023) 'The 2020 Chinese export control law: a new compliance nightmare on the foreign trade law horizon?', *China-EU Law Journal*, 8(3), pp. 81–95; https://doi.org/10.1007/s12689-021-00092-4.

Krolikowski, A., Hall, T.H. (2023) 'Non-decision decisions in the Huawei 5G dilemma: Policy in Japan, the UK, and Germany', *Japanese Journal of Political Science*, 24(2), pp. 171–189; https://doi.org/10.1017/S146810992200038X.

Lazarou, E., Lokker, N. (2019) *United States: Export Control Reform Act (ECRA)*. European Parliamentary Research Service. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/644187/EPRS_BRI(2019)644187_EN.pdf (Accessed: 13 December 2023).

Legrand, J. (1999) 'Some guidelines for fuzzy sets application in legal reasoning', *Artificial Intelligence and Law*, 7(2), pp. 235–257; https://doi.org/10.1023/A:1008357323873.

Lupovici, A. (2021) 'The dual-use security dilemma and the social construction of insecurity', *Contemporary Security Policy*, 42(3), pp. 257–285; https://doi.org/10.1080/13523260.2020.1866845.

Mahfoud, T., Aicari, C., Datta, S., Rose, N. (2018) 'The Limits of Dual Use', *Issues in Science and Technology*, 34(4), pp. 73–78.

Martins, B.O., Küsters, C. (2019) 'Hidden Security: EU Public Research Funds and the Development of European Drones', *JCMS: Journal of Common Market Studies*, 57(2), pp. 278–297; https://doi.org/10.1111/jcms.12787.

Maurer, S.M., Fischer, M. (2010) 'How to Control Dual-Use Technologies in the Age of Global Commerce', *Bulletin of the Atomic Scientists*, 66(1), pp. 41–47; https://doi.org/10.2968/066001006.

McCormick, D. (2006) 'Exports to China must not be used to develop the military [Asia Edition]', *Financial Times*, p. 13.

Meng, J.-H., Wang, J. (2023) 'The policy trajectory of dual-use technology integration governance in China: A sequential analysis of policy evolution', *Technology in Society*, 2023/72, p. 102175; https://doi.org/10.1016/j.techsoc.2022.102175.

Miller, S. (2018) 'Concept of Dual Use' in Miller, S. (ed.) *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Cham: Springer International Publishing, pp. 5–20; https://doi.org/10.1007/978-3-319-92606-3_2.

Mir, T.u.G., Wani, A.K., Akhtar, N., Shukla, S. (2022) 'CRISPR/Cas9: Regulations and challenges for law enforcement to combat its dual-use', *Forensic Science International*, 2022/334, 111274; https://doi.org/10.1016/j.forsciint.2022.111274.

Moore, G.J. (2023) 'Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies', *Journal of Chinese Political Science*, 28(1), pp. 151–167; https://doi.org/10.1007/s11366-022-09814-2.

Pillar, P.R. (2023) 'Export Controls and the Junction of Economics and National Security: A Review Article', *Political Science Quarterly*, qqad075; https://doi.org/10.1093/psquar/qqad075.

Puranik, T.G. (2021) 'The Impacts of Proliferation and Autonomy of Small Unmanned Aircraft Systems on Security' in Kosal, M.E. (ed.) *Proliferation of Weapons- and Dual-Use Technologies: Diplomatic, Information, Military, and Economic Approaches*. Cham: Springer International Publishing, pp. 33–52. [Online]. Available at: https://doi.org/10.1007/978-3-030-73655-2_4.

Pustovit, S.V., Williams, E.D. (2010) 'Philosophical Aspects of Dual Use Technologies', *Science and Engineering Ethics*, 16(1), pp. 17–31; https://doi.org/10.1007/s11948-008-9086-1.

Qi, Y., Chu, X. (2022) 'Development of the digital economy, transformation of the economic structure and leaping of the middle-income trap', *China Political Economy*, 5(1), pp. 14–39; https://doi.org/10.1108/CPE-09-2022-0012.

Rager-Zisman, B. (2012) 'Ethical and Regulatory Challenges Posed by Synthetic Biology', *Perspectives in Biology and Medicine*, 55(4), pp. 590–607; https://doi.org/10.1353/pbm.2012.0043.

Raivo, R., Trišč uka, J. (2023) 'The EU's control list of dual-use items has been updated', *Sorainen*, 27 February 2023. [Online]. Available at: https://www.sorainen.com/publications/the-eu-s-control-list-of-dual-use-items-has-been-updated/ (Accessed: 15 November 2023).

Rath, J., Ischi, M., Perkins, D. (2014) 'Evolution of Different Dual-use Concepts in International and National Law and Its Implications on Research Ethics and Governance', *Science and Engineering Ethics*, 20(3), pp. 769–790; https://doi.org/10.1007/s11948-014-9519-y.

Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (consolidated text) (2019) OJ L 079I, 21 March 2019. [Online]. Available at: http://data.europa.eu/eli/reg/2019/452/2021-12-23 (Accessed: 29 November 2023).

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (2021) OJ L 206, 11 June 2021. [Online]. Available at: https://eur-lex.europa.eu/eli/reg/2021/821/oj (Accessed: 19 September 2023).

Reinsch, W.A., Schleich, M., Denamiel, T. (2023) 'Insight into the U.S. Semiconductor Export Controls Update', *Center for Strategic & International Studies*, 20 October 2023. [Online]. Available at: https://www.csis.org/analysis/insight-us-semiconductor-export-controls-update (Accessed: 30 December 2023).

Ruohonen, J., Kimppa, K.K. (2019) 'Updating the Wassenaar debate once again: Surveillance, intrusion software, and ambiguity', *Journal of Information Technology & Politics*, 16(2), pp. 169–186; https://doi.org/10.1080/19331681.2019.1616646.

Rychnovská, D. (2016) 'Governing dual-use knowledge', *Security Dialogue*, 47(4), pp. 310–328; https://doi.org/10.1177/0967010616658848.

Sánchez-Cobaleda, A. (2022) 'Defining "dual-use items": legal approximations to an ever-relevant notion', *The Nonproliferation Review*, 29(1–3), pp. 77–95; https://doi.org/10.1080/10736700.2023.2202966.

Sarah, M., Andreas, R., Hakan, E. (2023) 'German proposal for Huawei curbs triggers telecom operator backlash', *Reuters* [Preprint], 20 September 2023. [Online]. Available at: https://www.reuters.com/business/media-telecom/german-interior-ministry-wants-force-5g-operators-slash-huawei-use-official-2023-09-19/ (Accessed: 30 October 2023).

Schmid, S., Riebe, T., Reuter, C. (2022) 'Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D', *Science and Engineering Ethics*, 28(2); https://doi.org/10.1007/s11948-022-00364-7.

Schneider, J., Meske, C., Kuss, P. (2024) 'Foundation Models', *Business & Information Systems Engineering*; https://doi.org/10.1007/s12599-024-00851-0.

Selgelid, M.J. (2009) 'Dual-Use Research Codes of Conduct: Lessons from the Life Sciences', *NanoEthics*, 3(3), pp. 175–183; https://doi.org/10.1007/s11569-009-0074-y.

Selgelid, M.J. (2013) 'Biodefense and dual-use research: the optimisation problem and the value of security', *Journal of Medical Ethics*, 39(4), p. 205; https://doi.org/10.1136/medethics-2012-100923.

Seyoum, B. (2017) 'National Security Export Control Regimes: Determinants and Effects on International Business', *Thunderbird International Business Review*, 59(6), pp. 693–708. [Online]. Available at: https://doi.org/10.1002/tie.21819.

Shagina, M. (2023) 'The Role of Export Controls in Managing Emerging Technology' in Berghofer, J. et al. (eds.) *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network*. Cham: Springer International Publishing, pp. 57–72; https://doi.org/10.1007/978-3-031-24673-9_4.

Skolnikoff, E.B. (2008) 'Responding to asymmetric threat: The dual-use strategy', *Dynamics of Asymmetric Conflict*, 1(1), pp. 42–47; https://doi.org/10.1080/17467580802054545.

Stone, M. (2012) 'Global Regulations for Dual-Use Research Tighten', *Bioscience*, 62(6), p. 616; https://doi.org/10.1525/bio.2012.62.6.17.

Stritzel, H. (2007) 'Towards a Theory of Securitization: Copenhagen and Beyond', *European Journal of International Relations*, 13(3), pp. 357–383; https://doi.org/10.1177/1354066107080128.

Taureck, R. (2006) 'Securitization theory and securitization studies', *Journal of International Relations and Development*, 9(1), pp. 53–61; https://doi.org/10.1057/palgrave.jird.1800072.

The State Council of China (2021) 'China's Export Controls' Xinhua, 29 December. [Online]. Available at: https://english.www.gov.cn/archive/whitepaper/202112/29/content_WS61cc01b8c6d09c94e48a2df0.html (Accessed: 15 December 2023).

The Wassenaar Arrangement Secretariat (2023) 'List of Dual-Use Goods and Technologies and Munitions List' *WA-List (23)1*, 1 December. [Online]. Available at: https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf (Accessed: 29 February 2024).

The White House (2023) *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 October 2023. [Online]. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (Accessed: 10 December 2023).

Thompson, K. (2024) 'How the Drone War in Ukraine Is Transforming Conflict, Council on Foreign Relations', *Council on Foreign Relations*, 16 January 2024. [Online]. Available at: https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict (Accessed: 11 February 2024).

Tongele, T.N. (2022a) 'Emerging & Foundational Technology Controls: A General Overview', *BIS 2022. Update Conference on Export Controls and Policy*, 29 June 2022. [Online]. Available at: https://www.bis.doc.gov/index.php/documents/2022-update-conference/3073-rev3-emerging-tech-update-2022-section-1758-controls-tongele/file (Accessed: 30 November 2023).

Tongele, T.N. (2022b) 'Emerging and Foundational Technology Controls', *AUECO – Export Controls and Research Security at Higher Education and Scientific Institutions*, 4 May 2022. [Online]. Available at: https://researchservices.upenn.edu/wp-content/uploads/2022/04/Emerging-and-Foundational-tech.pdf (Accessed: 30 November 2023).

Treaty on the Non-Proliferation of Nuclear Weapons (1968) Moscow, Russia, London, Washington, DC, 1 July 1968. [Online]. Available at: https://disarmament.unoda.org/wmd/nuclear/npt/ (Accessed: 15 November 2023).

UNODA (1972) *The Biological Weapons Convention*. [Online]. Available at: https://disarmament.unoda.org/biological-weapons/ (Accessed: 12 November 2023).

UNODA (2004) *UN Security Council Resolution 1540 (2004)*. [Online]. Available at: https://disarmament.unoda.org/wmd/sc1540/ (Accessed: 13 November 2023).

Urbina, F., Lentzos, F., Invernizzi, F., Ekins, S. (2022) 'A teachable moment for dual-use', *Nature Machine Intelligence*, 4(7), pp. 607–607; https://doi.org/10.1038/s42256-022-00511-6.

Vandenberghe, K. (2021) 'Dual-Use Regulation 2021/821: What's Old & What's New in EU Export Control', *Global Trade and Customs Journal*, 16(9) pp. 479–488; https://doi.org/10.54648/gtcj2021053.

Voetelink, J. (2022) 'International Export Control Law – Mapping the Field' in Beeres, R., Bertrand, R., Klomp, J., Timmermans, J., Voetelink, J. (eds.) *NL ARMS Netherlands Annual Review of Military Studies 2021: Compliance and Integrity in International Military Trade*. 1st edn. The Hague: T.M.C. Asser Press, pp. 69–94; https://doi.org/10.1007/978-94-6265-471-6_5.

The Wassenaar Arrangement Secretariat (2023) 'List of Dual-Use Goods and Technologies and Munitions List' *WA-List (23)1*, 1 December. [Online]. Available at: https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf (Accessed: 29 February 2024).

Weinberger, S. (2009) 'Export-control laws worry academics', *Nature*, 461(7261), p. 156; https://doi.org/10.1038/461156a.

Whang, C. (2021) 'Trade and Emerging Technologies: A Comparative Analysis of the United States and the European Union Dual-Use Export Control Regulations', *Security and Human Rights*, 31(1–4), pp. 11–34; https://doi.org/10.1163/18750230-31010007.

The White House (2023) *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. 30 October 2023. [Online]. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (Accessed: 10 December 2023).

World Economic Forum: Centre for the Fourth Industrial Revolution (2023) 'Top 10 Emerging Technologies of 2023' *Geneva: World Economic Forum*, 26 June. [Online]. Available at: https://www3.weforum.org/docs/WEF_Top_10_Emerging_Technologies_of_2023.pdf (Accessed: 25 October 2023).

Yoo, C.S., Mueller, A. (2024) 'Crouching Tiger, Hidden Agenda? The Emergence of China in the Global Internet Standard-Setting Arena', *Federal Communications Law Journal*, 76(2), pp. 143–215.

Yoshizawa, G., Shinomiya, N., Kawamoto, S., Kawahara, N., Kiga, D., Hanaki, K.I., Minari, J. (2023) 'Limiting open science? Three approaches to bottom-up governance of dual-use research of concern', *Pathogens and Global Health*, 118(4), pp. 285–294; https://doi.org/10.1080/20477724.2023.2265626.

Zwartkruis, W. (2024) 'Foreign Direct Investment and Security: What is Actually the Problem?' in Hillebrand-Pohl, J., Papadopoulos, T., Wiesenthal, J. (eds.) *National Security and Investment Controls*. 1st edn. Cham: Springer Nature Switzerland, pp. 1–32; https://doi.org/10.1007/17280_2024_29.

Chopping the Red Tape (1998) *Business Europe*, 38(17), pp. 4–5.

Deemed exports (no date) *Bureau of Industry and Security*. [Online]. Available at: https://www.bis.gov/deemed-exports (Accessed: 25 January 2024).

Deemed Exports and Fundamental Research for Biological Items (2024) *Bureau of Industry and Security*. [Online]. Available at: https://www.bis.doc.gov/index.php/policy-guidance/product-guidance/chemical-and-biological-controls/14-policy-guidance/deemed-exports/111-deemed-export-and-fundamental-research-for-biological-items (Accessed: 30 January 2024).

Final Document of the BWC Sixth Review Conference (2006). [Online]. Available at: https://bwc1972.org/publication/final-document-of-the-bwc-sixth-review-conference-2006/ (Accessed: 15 September 2023).

The International Traffic in Arms Regulation (ITAR) (2024) *Directorate of Defense Trade Controls*. [Online]. Available at: https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987 (Accessed: 19 February 2024).

Missile Technology Control Regime Guidelines (2023) *MTCR*. [Online]. Available at: https://www.mtcr.info/en/mtcr-guidelines (Accessed: 10 December 2023).

Nuclear Suppliers Group Guidelines (no date) *Nuclear Suppliers Group*. [Online]. Available at: https://www.nuclearsuppliersgroup.org/index.php/en/guidelines/nsg-guidelines (Accessed: 15 November 2023).

Officials Show Scant Interest in Major Export Control Overhaul for China (2011) *Inside US Trade*, 29(38). [Online]. Available at: https://www.proquest.com/trade-journals/officials-show-scant-interest-major-export/docview/913046784/se-2 (Accessed: 29 September 2023).

Supplement No. 4 to Part 744, Title 15. Entity List (2024) *Code of Federal Regulations*. [Online]. Available at: https://www.ecfr.gov/current/title-15/part-744/appendix-Supplement No. 4 to Part 744 (Accessed: 21 March 2024).

The United States Announces Export Controls to Restrict China's Ability to Purchase and Manufacture High-End Chips (2023) *The American Journal of International Law*, 117(1), pp. 144–150; https://doi.org/10.1017/ajil.2022.89.

United States: Proposed Changes to the EU Dual-Use Export Control Regime (2016) *MENA Report*. [Online]. Available at: https://www.proquest.com/wire-feeds/united-states-proposed-changes-eu-dual-use-export/docview/1824526908/se-2 (Accessed: 15 September 2023).

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1995). [Online]. Available at: https://www.wassenaar.org/ (Accessed: 25 November 2023).

IV.2

MILITARY AND DEFENCE ISSUES OF ARTIFICIAL INTELLIGENCE

Chapter 8

The Use of Artificial Intelligence-Enabled Systems by Modern Armed Forces and Some Related Concerns

Iztok Prezelj

Abstract

Artificial intelligence (AI) is a new technology permeating several civilian and military aspects of human life. In the military and defence sectors, it is regarded as a game-changing technology that will affect the distribution of strategic power among major countries and improve efficiency at the tactical level by performing various specialised tasks. This paper tests and confirms the hypothesis that the emergence of AI introduces new possibilities to improve military and defence capabilities (benefits), alongside a broad range of concerns, challenges, and risks. This paper positions AI as a wave of revolution in military affairs, analyses a broad spectrum of potential and actual applications of AI by armed forces and defence establishments, and identifies several geopolitical and strategic concerns related to the development and use of AI systems. Based on these identified concerns, several regulatory approaches are proposed in the conclusion.

Keywords: Artificial intelligence, autonomous weapon systems, intelligence, defence, geopolitics, challenges, revolution in military affairs (RMA), power struggle

Iztok Prezelj (2024) 'The Use of Artificial Intelligence-Enabled Systems by Modern Armed Forces and Some Related Concerns'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 357–394. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_8

1. Introduction

New technologies have always brought a large spectrum of new possibilities and risks simultaneously. Artificial intelligence (AI) is a new form of technology that has been present in civil life for a relatively long time. For example, Amazon and Google have been using these tools to predict the needs of their customers, and Cambridge Analytica used it to target and influence voters in many elections. Deep Blue has beaten the chess world champion, and DeepMind's AlphaGo the world champion in GO in 2016. A large, statistically based language model (ChatGPT) was launched for testing and use by the global public. AI is not only a future scenario but is already present in all dimensions of our lives, in various applications and industries, including defence and military sectors. AI complements and extends human capabilities to a degree unimaginable until recently. Driven by data and algorithms, AI affects almost every aspect of our lives.[1]

AI quickly penetrated the armed forces and defence establishments. The development of armed forces and ways of warfare, including military tactics, doctrines, and strategies, has been largely driven by the development of technology. Technology has been at the heart of all revolutions in military affairs and military transformation processes in the history of the armed forces. The first known use of AI in the armed forces in the sense of complete control of a military system by AI occurred in 2016 when the U.S. Air Force used the AI algorithm to completely control the sensor and navigation systems on the U-2 Dragon Lady spy plane during a training exercise.[2]

However, there is no universally accepted definition of AI. Generally, AI refers to the ability of a computer or computer-controlled robot to perform tasks commonly done by humans, such as the ability to reason, discover meaning, generalise, solve problems, learn from past experiences, and adapt to new circumstances.[3] Another definition says that it is an umbrella term that covers automating decision-making processes that traditionally require the use of human intelligence, such as recognising patterns, learning from experience, drawing conclusions, making predictions, and taking actions. Driven by sensors and data digitalisation, AI can predict outcomes, thereby enabling better data-driven decisions. Research on AI has predominantly focused on learning (e.g. by trial and error, storing the solution for the next iterative situation), inductive and deductive reasoning (e.g. drawing inferences), problem-solving by searching through a range of possible actions to reach predefined goals or solutions, perceptions in the sense of scanning the environment, and language processing by building large language models (e.g. ChatGPT). The earliest work on AI was done by Alan Turing, a British logician and crypto analyst who was also involved in military intelligence deciphering activities in Bletchley Park in the

1 Thiele, 2021b, p. 76.
2 See: Nurkin, 2023, p. 37.
3 Copeland, 2023; Luberisse, 2023a, p. 2.

UK during World War II. He envisioned machines with scanners that move back and forth through the memory, learn from experience and possibly alter their own instructions. The Turing test is where, if a machine can engage in a conversation with a human without being detected as a machine, it has demonstrated human intelligence.[4]

The purpose of this paper is to analyse the use of AI by modern armed forces as a potential strategic game-changer in regional and global geopolitical contexts. This paper aims to embed AI in the academic narrative of the revolution in military affairs (RMA), identify and analyse a broad spectrum of potential or actual uses of AI by armed forces and defence establishments, and identify several geopolitical and strategic concerns about developing and using AI systems. In conclusion, we identify the key areas that require a lucid regulative approach if we want the transition to the use of AI to avoid creating further instabilities or even wars. This paper focuses on AI systems that can be used by modern armed forces, not artificial general intelligence (AGI) or strong AI. Applied AI involves advanced information processing aimed at developing commercially viable and targeted smart systems. In practice, the application of such expert systems has been much more successful than AGI. Good expert systems are often better than single human experts, and their scope of application can be substantial.[5]

In this paper, we hypothesise that the emergence of AI has introduced new potential to improve military and defence capabilities (benefits) and, simultaneously, a broad range of concerns, challenges, and risks. The goal of society should be to strike an appropriate balance between the potential benefits and risks. However, there are several important questions related to the organisational, technical, and functional integration of AI-enabled systems that need to be answered and properly regulated.

In this early stage of AI development, we first need to learn about the actual capabilities of AI to discuss its limitations and regulation. In the military field, AI is regarded as one of disruptive technologies that can change everything. It was developed to address the need to handle an increasing quantity of data from an increasing number of sensors on the battlefield. Sources depict AI as a game-changing technology, as not a single technology breakthrough,[6] as a transformative technology that has the potential to shape and revolutionise our world in countless ways.[7] AI is driven by an exponential increase in computational power, faster processing power, larger datasets (big data), and the increased availability of large amounts of data. This has allowed the development of advanced machine-learning algorithms that can process vast amounts of information and make accurate predictions and decisions.[8]

4 Ibid.
5 For distinction between AGI and AI expert systems see Copeland, 2023.
6 Schmidt et al., 2021, pp. 1–7.
7 Luberisse, 2023a, p. xiii.
8 Ibid., p. 3; Copeland, 2023.

2. AI as a Game Changer in the Military Dimension

AI has been increasingly used in the modern armed forces. Several authors have stressed that modern technologies are game-changers in modern warfare,[9] and we should know that AI is not a weapon in itself; it is an enabler or enabling technology, much like electricity or the combustion engine or the Internet. These are all technical achievements that have influenced all spheres of human life in manifold and contradictory ways. The impact of AI will depend on particular applications, and is best understood as a cluster of enabling technologies that can be applied to most aspects of the military sphere. It also does not make sense to view AI as an isolated technology, because of its manifold interactions with other technologies.

Similar to other new technologies, AI can bring changes to warfare and enable a revolution in military affairs. The concept of the military-technical revolution (MTR) was introduced in the 1980s by Soviet general staff writers who argued that a new range of technological innovations (microprocessors, computers, lasers, electronics, kinetic energy, enhanced accuracy, range, and lethality of weapons) and related Western doctrinal innovations constituted a fundamental discontinuity in the nature of war, which they dubbed the MTR. Approximately a decade later, this Soviet approach was upgraded by U.S. writers into a new concept – the revolution in military affairs (RMA). This concept criticised the narrow approach of MTR and emphasised that changes in military affairs included not only technological aspects but also organisational, structural, doctrinal, and operational changes.[10] A second aspect of this concept was the revolutionary changes in military affairs, interpreted as profound, radical, discontinuous, non-incremental, and possibly disruptive.[11] The revolutionary image of the changes was stimulated by fascinating images from the 1991 Gulf War and the wars in former Yugoslavia, Iraq, and Afghanistan. The term 'revolution in military affairs' has become fashionable; according to Horowitz and Rosen, it is a promotional slogan associated primarily with selling new pieces of technology. Anything associated with this appears to be good and promising.[12]

Technological advances have resulted in significant changes in warfare. Four aspects of the RMA have been discussed in the literature: RMA I (emerging from the second half of WWI in the form of combat vehicles), RMA II (based on the insurgent method of war in Asia), RMA III (focused on the use of nuclear weapons and other long-range means of delivery in the Cold War), and IT-driven RMA IV (focusing on digitalisation, including computers, precision-guided munitions, active and passive sensors, cyberspace, C4, and robotics). The RMA V is the next aspect revolution that

9 Thiele, 2021a, p. 59.

10 Cooper, 1994, p. 1; Davis, 1996; Horowitz and Rosen, 2005, p. 447; Hundley, 1999, pp. 11–17; MacGregor and Murray, 2001, p. 12; Krause, 1997, p. 18; Raska, 2011.

11 Horowitz and Rosen, 2005, p. 441; Osinga, 2010, p. 14; Roxborough, 2002, p. 71; Sheehan, 2008, p. 14.

12 Horowitz and Rosen, 2005, p. 440.

will be brought about by new technologies. Modern hybrid warfare[13] will use a creative mix of RMA I to RMA V tools to achieve its objectives.[14] IT-driven RMA, which lasted from the 1970s to the 2010s, was characterised by the superiority of the West (primarily the U.S.), while in AI-driven RMA, this primacy was challenged by China. A real military technological tsunami is on the way that may differ from previous RMAs.[15]

Discussion on the use of AI normally gets narrowed to discussion between the "boomers", enthusiastically supporting the fast introduction of AI into practice, and "doomers", focusing on challenges and risks, and advocating for AI to be strongly regulated. Another classification of the use of AI in the military domain has identified three perspectives on its influence on the characteristics of war. "Enthusiasts" stress that AI will revolutionise warfare, influence the character, nature and tempo of war and give decisive advantages to adopters. "Deniers" believe that AI is too immature to be used by militaries and that hurdles for its effective implementation, such as technological, organisational, socio-political, ethical, and legal, are too high. Without new operational concepts and organisational structures, technology will not be able to fundamentally influence the war. Finally, "pragmatics" believe that AI will find an evolutionary (not revolutionary) way to the battlefield, but it will not change the immutable nature of war and will only impact the operational and tactical levels of war, while strategy development will mainly remain a human endeavour.[16]

Nonetheless, AI will enable militaries to operate faster and with greater accuracy, and has three key application areas in armed forces: interpretation of increasing amounts of data, increasing the speed of warfare (through increasing the speed of the Observe, Orient, Decide and Act (OODA) loop) especially in decision-making, and battlefield applications, such as swarms or the "loyal wingmen" idea.[17] AI has the power to unlock the full potential of data, making existing products and systems more intelligent, and learning, adapting and acquiring new skills based on its ability to find structures and patterns in data.[18] Consequently, AI has the following key operational benefits: superior decision-making through actionable data and information; a reduction in administrative and staff work through predictive logistics;[19] and improved ISR capabilities and risk reduction through autonomous systems.[20]

13 Hybrid warfare is the combination of a broad spectrum of military and non-military instruments of power, such as politics, the military, diplomacy, economics, information, technology and society, which operates in the grey areas between war and peace, friend and foe, domestic and foreign relations, civilian and military. (see: Schmid, 2021, p. 12).

14 Thiele, 2021a, pp. 65–69.

15 Raska and Bitzinger, 2023, pp. 1–2.

16 Rickli and Mantellassi, 2023, pp. 12–13.

17 Horowitz, 2018, pp. 3–4.

18 Thiele, 2021b, p. 76.

19 The use of increasingly autonomous systems will also contribute to reduction of military personnel in staffs and on the battlefield.

20 Thiele, 2021e, p. 190.

One should also stress that AI is a dual-use, often open source, and rapidly diffusing technology. AI has increased the complexity of warfare, but it offers a broad spectrum of possibilities for reducing human workload and providing superior capabilities to complement individual human work. AI-enabled autonomous tools will become useful teammates for human beings. Because of AI, human-machine teams will be better able to perform their functions.[21]

2.1. An Example of Fast Implementation of Artificial Intelligence by Ukraine in the Data-Driven Combat

It is not well known that the Ukrainian military rapidly applied certain elements of AI after the attack by Russia. Ukraine has reached faster than NATO member states: the fusion of data from all available sources and AI-assisted analysis of the data, the creation of a comprehensive situation picture, and AI-aided vehicle or target identification, with prioritisation, and allocation of targets streamed into different weapon systems. The best example of this is the Kropyva app, which is installed on Android tablets and provides Ukrainian troops with an up-to-date picture of the situation. Other significant software, artificial neural networks, and machine learning systems used by the Ukrainian Armed Forces have been rapidly developed, tested, and deployed. Development, testing, and learning of AI algorithms is conducted during battles. Artificial neural networks are used to identify patterns in datasets, whereas machine learning is based on an ever-growing dataset. The data enters the system from military intelligence gathering and intelligence agencies, physical reconnaissance operations, military and commercial satellite imagery, drone flights, cell phone photos and videos, and open source intelligence. Incorporating all available disparate sources and fusing the data gives Ukrainian forces an edge in situational awareness, improves decision-making for military leaders, and simultaneously enables high mobility and precision. Ukrainian combat, tactics and strategy are driven by data and analytics. This implies that artificial neural networks for rapid pattern recognition in complex data and machine learning have become a permanent and integral part of warfare.[22] Despite all this, Ukraine could not change the direction of the war, and AI turned out not to be a game changer yet.

21 Mashur, 2019, p. 4, cited in Thiele, 2021b, p. 76.
22 Lange, 2023, pp. 12–14.

3. Identification and Analysis of a Broad Spectrum of Potential and Actual Use of Artificial Intelligence by Armed Forces and Defence Establishments

This chapter demonstrates that the potential use of AI spans the entire spectrum of military and defence activities. Specific typical fields of application were identified and analysed (see Figure 1).

AI in the armed forces serves as an analytical enabler, disruptor, and force multiplier. As an analytical enabler, AI can provide quicker, more accurate, and reliable data analysis of much larger datasets, and assisting decision systems (command and control). As a disruptor, AI automatises, democratises, and sophisticates the creation and spread of disinformation and propaganda, thus providing affordable and impactful technology for any actor. AI-enabled disinformation and misinformation will erode trust in democratic institutions and processes, sowing confusion and polarisation among people. As a force multiplier, AI is increasing the autonomy of sophisticated weapon systems, such as killer robots, drone swarms, and mass surveillance tools.[23]

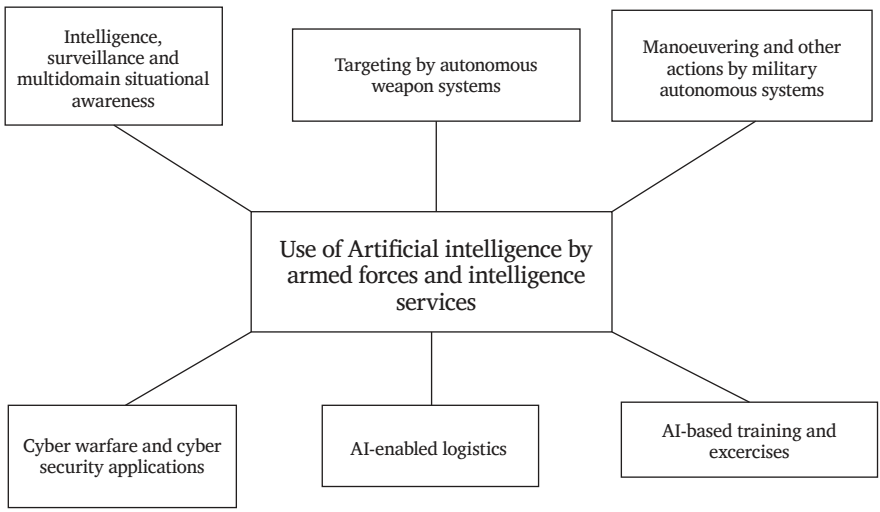
AI will contribute to military applications at tactical and strategic levels by analysing big data, optimising processes, and supporting planning. AI-enabled systems are capable of multitasking and can collect categorise, and transmit data, signals, images, and videos collected by drones.[24] This will accelerate the decision-making process and lead to the achievement of multi-domain situational awareness using any available data source in a structured manner.[25] Virtual teammates support human analysts in understanding complex information.[26] Additionally, AI can be used in both offensive and defensive systems. In fact, it is difficult to distinguish between exclusively defensive and exclusively offensive AI applications, as in physical military systems. AI-generated weapons have stimulated the development of AI-generated defence systems.

The central focus of AI is machine learning (i.e. learning from data without explicit programming). Machine learning requires a large amount of data. The more data that an AI system contains, the more accurate it is. Mashur stressed that machine learning-enabled software must first be trained by experts, preferably using large datasets. This enables the algorithms to generate predictions independently of unknown data.[27] Defence and security organisations use machine learning and visioning software to permanently update knowledge about the operational environment. New capabilities have emerged with the introduction of deep learning,

23 Rickli and Mantellassi, 2023, p. 13.
24 Mashur, 2019, cited in Thiele, 2021b, p. 77.
25 Horowitz, 2018, cited in Thiele, 2021, p. 77.
26 Thiele, 2021b, p. 78.
27 Mashur, 2019, p. 1.

combined with the free availability of large amounts of data and increased processing ability.[28] The development of AI systems significantly depends on experimentation; only those AI technologies that will be experimentally proven and successfully applied in hybrid warfare will enter the standard inventory of the armed forces.[29]

Figure 1: Typical use of Artificial intelligence by Armed Forces and Intelligence Services.



3.1. Intelligence, Surveillance and Multi-Domain Situational Awareness: Use of AI in Predictive Analytics for Discovering Threats and Improving Decision-making

AI also offers predictive analytics, making it an analytical enabler for the armed forces. Analytics is one of the most promising dimensions of military applications. AI is effective in the analysis of large datasets, such as drone footage or thousands of pages of text. AI can digest, categorise, and analyse more data than human analysts, and it may also find correlations in data that escape the human mind. AI systems will become increasingly capable of analysing connections between data points, flagging suspicious activities, spotting trends, fusing separate data elements, mapping networks, and even predicting future behaviours and trends.[30] Pooling vast quantities of information, such as messages, reports, charts, spreadsheets, telephone records, and sensor data will improve the detection of unseen patterns in the data. This will make intelligence information more actionable, and will increase operational tempo

28 Mashur, 2019, p. 4; Thiele, 2021e, p. 188.
29 Roy, 2004, cited in Thiele, 2021b, p. 72.
30 Horrowitz, 2018, cited in Rickli and Mantellassi, 2023, p. 19.

and targeting, improve the assignment of scarce resources, and help form coherent proposals.[31] Its enormous capacity for analysis and evaluation is strongly associated with big data.[32] In near real time or even in real-time situations, AI will vastly increase the agility of the forces involved in manoeuvring and responding.[33]

In hybrid warfare, political and military decision-makers can only make accurate decisions if they comprehensively understand the operational environment, including all relevant domains. They require adaptive and agile situational awareness in order to act in a targeted and effective manner. A wealth of sensors, technologies, big data, AI, evaluation algorithms, and quality open source information can be used to generate and provide comprehensive situational pictures that portray patterns of life, human terrain, and anomaly detection. Emerging technologies such as advanced modelling, big data analysis, AI and machine learning are instrumental in building a cross-domain capability to tackle hybrid challenges and generate adaptive and agile multi-domain situational awareness.[34] In this respect, it is very valuable that AI can enable faster and real time data transfer across military systems, for example, from air systems (drones) to ground systems (artillery), instead of existing time-consuming "translations" at various interfaces.[35]

AI predictive analytical models can identify trends and patterns within a dataset to predict the likelihood and timing of a trend. Predictive analytic models can correlate signs of preparation for unlawful activities, allowing intelligence agencies to intercept an act before the plot unfolds. For example, the CIA, FBI, and U.S. armed forces use Palantir's predictive analytics software to pool and analyse data from various state sources[36] and create action options to be selected by decision-makers and military commanders.[37] By correlating information, predictive analytics models may support the search for signs of planned criminal or terrorist attacks, such as purchasing weapons or bomb-making materials.[38] Palantir's product, Palantir Defense, can help analyse and sort large volumes of diverse data from numerous sources (e.g. unstructured message traffic, structured identity data, charts, spreadsheets, telephony, documents, network data, sensor data, and full-motion videos) to alert users of possible relationships indicative of suspicious behaviour worth monitoring using predictive analytics. Users can make operational plans and strategic decisions based on the patterns present in unsynchronised data. For example, an AI machine

31 Thiele, 2021b, p. 78.

32 Big data is characterized by the three Vs: Volume – massive size of data, generated by all kinds of sources, Velocity – fast data generation by online systems and sensors, and Variety – different types of data, structured, semi-structured or unstructured. With a view of hybrid contingencies, two additional Vs are important: Veracity – whether the data is intentionally manipulated and Visualisation – the best way to enable informed decisions in a Big data/AI environment. Thiele, 2021c, p. 136.

33 Thiele, 2021a, p. 64.

34 Thiele, 2021c, p. 135.

35 Mashur, 2019, p. 3.

36 Roth, 2019a.

37 See: https://www.palantir.com/platforms/gotham/ (Accessed: 5 January 2024).

38 Roth, 2019, cited in Thiele, 2021e, p. 189.

learning model can be trained on millions of emails recovered from people before they carry out an attack. The AI model learns based on this training to discern dangerous patterns based on specific words, phrases, or times and makes predictions. Sources indicate that Palantir was successfully used to uncover the infamous terrorist leader, Osama bin Laden.[39] It is possible that the CIA might be using Stabilitas to gauge stability and safety in regions around the world.[40] This software helps predict social unrest in a region using sentiment and predictive analytics. Its AI model has been trained on thousands of online news articles, weather reports, social media, and private database entries labelled as unsafe environments (riots, killings, political upheavals, or natural disasters). The labelled text data then runs through the AI software learning algorithm to train it to discern dangerous indications. A user can ask the system to provide information about social unrest in any particular region, and Stabilitas offers results with a certain confidence interval on how likely the identified violent events are to correlate with additional violent events of the same nature in the future.[41] According to OnSolve,

> Stabilitas' AI solution constantly ingests more than 17,000 global data sources to identify nearly 300.000 critical events each day, such as natural disasters and geopolitical incidents. The solution then identifies the people, facilities, assets, and operations impacted by those events in real time. This allows decision-makers to effectively monitor and confidently respond to the multitude of natural and man-made incidents that endanger lives and pose billions of dollars in risk to organizations each year.[42]

AI can support analysis from top-level political decision-makers down to the infantry soldiers in the field. AI has the potential to predict the behaviour of foreign states and societies, predefine policy options, and generate highly complex simulations related to the ongoing crisis in real time. This means AI can facilitate greater precision, complement human assessments and predictions, and accelerate decision-making processes.[43]

The intelligence community can benefit from AI more than any other national security subsystem. Sources argue that the IC should integrate AI-enabled capabilities across all aspects of its work, from collection to analysis, including more open source and publicly available information, prioritising the collection of scientific and technical intelligence. Intelligence agencies must also develop innovative solutions for

39 Roth, 2019c.
40 Roth, 2019a.
41 Roth, 2019c.
42 See: OnSolve Announces Acquisition of Stabilitas, an AI-driven Intelligence Platform for Situational Awareness. [Online]. Available at: https://www.onsolve.com/latest-news/onsolve-announces-acquisition-of-stabilitas (Accessed: 9 January 2024).
43 Mashur, 2019, p. 2.

human-machine teams to augment human judgement.[44] AI will be usable across the intelligence spectrum of the military, defence, and civil agencies. For example, the CIA, as a civilian agency, likely uses AI to discover threats and thwart planned attacks, neutralise cyberattacks through email, survey areas via satellite, and identify and predict social unrest in a region.[45]

Let us consider the United States as an example. U.S. sources stress that AI-enabled technologies or capabilities will improve every stage of the intelligence cycle, from tasking to collection, processing, exploitation, analysis, and dissemination. Increasing the number of sensors will increase the volume, velocity, and variety of data, challenging analysts to perform their jobs. AI will help the IC find needles in haystacks, connect the dots, and disrupt dangerous plots by discovering trends and previously hidden or masked indications or warnings. AI algorithms can sift through vast amounts of data to find patterns, detect threats, identify correlations, and make predictions. AI can identify correlations between open source data and other sources of intelligence. This enables data fusion from dissimilar data streams to create a composite picture. This enhances the all-domain awareness and leads to more informed decision cycles.[46] The U.S. goal is to make its IC AI-ready by 2025. Intelligence professionals will have baseline digital literacy and access to the digital infrastructure and software required for full AI integration at each stage of the intelligence cycle. The IC should automate each stage of the cycle to the greatest extent possible. Intelligence products will be in both human-readable and automated machine-readable versions, which can be utilised by any analytical system in the IC. Products should be disseminated at machine speed in both formats mentioned above. Once individual intelligence disciplines are automated, the IC should fuse these processes into a continuous pipeline of all source intelligence analyses.[47] The U.S. military uses AI for intelligence, surveillance, and reconnaissance platforms and sensors. This enables the use of unstructured data sources, including full-motion videos, or approaches comparable to the automated exploitation of audio and text. This improves understanding of behavioural patterns, structures, and processes and dramatically reduces reaction times.[48] It has the potential to accelerate decision-making because it enables security-related developments to be analysed faster and better than before.[49] AI could also gather information during the security clearance process.[50] The armed forces acquire enormous amounts of data daily from various sources such as satellite footage, UAVs, video surveillance, and phone cameras. The challenge is not so much collecting the data, but processing it for strategic information. Machine vision software has the potential to sort large amounts of data faster than trained human

44 Schmidt et al., 2021, p. 10.
45 Roth, 2019c.
46 Schmidt et al., 2021, pp. 109–110.
47 Schmidt et al., 2021, pp. 110–111.
48 Egel et al., 2019, cited in Thiele, 2021e, p. 188.
49 Merz, 2019, cited in Thiele, 2021e, p. 189.
50 Schmidt et al., 2021, p. 114.

analysts. In the U.S., the Department of Defense's (DoD) Project Maven represents an attempt to use AI to categorise large sums of surveillance data. Sources stress that the AI, in this case, was trained on 36 different types of objects (e.g. cars, weapons, and persons) by screening hours of footage from various angles and under various lighting conditions. When the system encounters new footage, the algorithm can determine its content, identify anomalies, and alert a human operator. Several applications of this approach have been tested on satellite images (for example, Orbital Insights are linked together with a large amount of satellite imaging data from various networks to assemble high-definition images, taking the most useful pieces of each and removing clouds, smog, and weather effects from the images.[51] The product counts and measures roads, aircraft, clouds, smog, haze, lakes, land, buildings, oil tanks, vehicles, and other objects; tracks their movements by knowing the normal activity patterns; detects anomalies; and aids in mission planning. Its AI software was trained on millions of satellite images of the Earth's surface captured at various angles, altitudes, weather patterns, and lightning conditions. It is also likely to be used by CIA.[52]

3.2. Targeting by Autonomous Weapon Systems

Targeting is the process of identifying, selecting, and engaging individuals, groups, and movable or unmovable objects to kill or destroy in military or counterterrorism operations. Roth stressed that targeting is increasingly judged by the accuracy and speed it can lock onto targets. Weapon platforms primarily become autonomous when they are able to identify and track targets in a given space. Currently, no autonomous weapons platforms are designed to fire ordnance without the approval of a monitoring operator. The AI behind the targeting will need to be trained to know what exactly is a strategic target worth focusing its firepower on, and alerting the human operator to monitor the platform. Platforms that use AI for targeting are drones, air defence systems (targeting mostly rockets before hitting the targets), tanks (in tank turrets, e.g. RAPIDFire), handheld missile launchers, and naval missiles. All these systems will be trained to avoid defensive countermeasures by the attacked systems (for example, allowing the missile to react to evasive manoeuvres of the target and still connect to its target).[53] AI also assists with weapons in the cybersphere. For example, Lockheed Martin's Behavioural Learning for Adaptive Electronic Warfare (BLADE) is meant to attack and disable the wireless communication networks of enemy systems using AI. BLADE can predict countermeasures by the target and adapt, leading to the disabling of wireless communication signals, including remote phone signals aiming to detonate an improvised explosive device.[54]

51 Roth, 2019a.
52 Roth, 2019c.
53 Roth, 2019a.
54 Roth, 2019a.

A special case of an autonomous weapons system is the loitering munition. Loitering munitions can independently acquire and engage targets in given geographic areas of operation. Currently, geographical area, loitering time, and target category are generally determined by humans.[55]

3.3. Manoeuvring and Other Actions by Military Autonomous Systems

AI has already entered several weapon systems and other technical platforms in the armed forces and will increasingly enter them. Mini-, micro-, and nano-unmanned autonomous vehicles are being developed in the aerial, surface, undersea, and ground domains. These systems use AI to perform tasks previously performed by humans. AI provides core technologies for machine learning and cyber security, which are essential for the further development and deployment of autonomous systems.[56]

One useful application of autonomous vehicles is in patrolling. They can patrol secure areas, investigate any signs of intruders, and alert human security forces. This leads to a significant reduction in human patrols, and creates opportunities for the force to focus on more valuable tasks.[57] Another example is the U.S. Army Expedient Leader-Follower composition of convoys, in which only the first vehicle is manned.[58] Another example in which tests have shown that AI systems are, in some cases, already performing better than humans is the case of robotic air-to-air refuelling: unmanned airplanes manage to keep themselves steady in difficult weather where human pilots are struggling. Another example is that some AI pilots have begun to win duels in dog fights over their human counterparts in war games.[59]

Drones are one of the main focuses of AI integration. The goal is to create drones that fly without human operators and achieve comparable performance. Thus, the operators will be able to focus on more pressing activities. For example, military units can check whether they are being pursued potentially saving lives.[60] The trend is to have swarms of autonomous systems connected to each other and to a human controller. Drone swarms are a collection of autonomous robots that react to the battlefield and act as a single integrated weapon system with the ability to self-organise.[61] Another definition is that the swarming of drones involves 'several to several dozen or even hundreds of networked autonomous drones linked through distributed decision-making rules that allow parts of the swarm to operate in conjunction with one another and be independent of central control'.[62] Israel was the first country to

55 Rickli and Mantellassi, 2023, p. 22.
56 Thiele, 2021f, p. 197.
57 Roth, 2019a.
58 Mashur, 2019, p. 4.
59 Gatopoulos, 2021, p. 4.
60 Roth, 2019b.
61 See: Rickli and Mantellassi, 2023, p. 23.
62 Nurkin, 2023, p. 49.

employ intelligent drone swarms. In the summer of 2021, they used them in the conflict with Hamas in Gaza for intelligence, surveillance, and reconnaissance.[63] The AI ensures that the flight-control systems of entire swarms can be orchestrated and that sensor data will be processed in real time. These swarms require advanced machine learning. AI supports both semi-autonomous and autonomous systems. For example, the U.S. Air Force's future long-range strike aircraft set to replace the B-2 stealth bomber will be able to operate with or without a crew. Unmanned trucks and other supply vehicles have been designed to perform dirty, dull and dangerous battlefield tasks.[64] Russia is expected to build large nuclear-powered unmanned submarines that are theoretically, capable of carrying nuclear weapons. Russia and China are also focusing on unmanned robot tanks, with Russia testing the latest version in Syria,[65] and the U.S. is experimenting with autonomous drones, submarines, and aircraft.

Human-machine teaming will become critical in future AI-enabled military realities. Human-machine teaming refers to teams of human and un-crewed systems connected to and operating in close conjunction with one another to carry out missions that cannot be performed independently.[66] In future conflicts, unmanned autonomous systems will act as part of a team, closely connected to human decision-makers and emergency services. Generally, drones take over boring tasks, whereas humans maintain command of control functions and concentrate on cognitively demanding tasks. It can be assumed that a manned system will be escorted by swarms of unmanned systems.[67] Such weapon systems can have three levels of autonomy: human-in-the-loop, human-on-the-loop, and human-out-of-the-loop. Currently, human-in and on-the-loop exist and are deployed.[68] There is increasing tension between the need for speed and the need for human control of lethal force against other humans, and this relationship will determine the future of convergence in this field.[69] Finally, this link between humans and robotic platforms will be targeted in war time and potentially cut off by enemy forces. The head and body would be separated, and the question is, what happens next? For example, the U.S. Global Hawk is structured to carry out orders without a vulnerable data link. The U.S. concept of Loyal Wingmen would also be based on the AI bodyguard principle, where the robot would defend the manned aircraft and sacrifice itself, if necessary, to save the human pilot.[70] In addition, single pilots will be able to control squadrons

63 Ibid., p. 50.
64 Thiele, 2021f, p. 200.
65 See: Thiele, 2021f, p. 202.
66 Nurkin, 2023, p. 37.
67 Thiele, 2021f, p. 200.
68 Rickli and Mantellassi, 2023, p. 22.
69 Nurkin, 2023, p. 51.
70 Gatopoulos, 2021, pp. 4–5.

of unmanned aircraft, contributing to a decrease in the number of crew members.[71] The use of these systems is expected to increase significantly.

The use of AI will enable forces to expand their warfighting capacity without increasing manpower or providing a force multiplier where the same number of people can do and achieve more. Such robotic platforms will perform tasks considered too menial or dangerous for humans, such as unmanned supply convoys, mine clearances, and air-to-air refuelling.[72] However, all these benefits will also proliferate outside legitimate and legal security systems as they become increasingly available to irregular actors, such as terrorists and criminal organisations.

3.3.1. A special case of Autonomous Nuclear Weapon Systems

Nuclear weapon systems will also become AI-capable. AI in these systems will significantly improve response speed and accuracy. Therefore, it is important to reduce the time required to detect and respond to nuclear threats. An AI-enabled example is the Russian nuclear automated defence system Perimetr, which can detect a nuclear strike against Russia and launch a retaliatory nuclear strike even if the lines of communication with strategic missile forces are destroyed. The system analyses a broad spectrum of data, such as seismic activity, radiation levels, atmospheric pressure, and the volume of chatter on military radio frequencies. The system decides to launch a retaliatory strike after approval by the human commander, but in the case of a failure in communication with the command centre, it can launch such a strike alone. Additionally, it can launch a command rocket in the air over Russia, and retaliatory strike activation from all available platforms (silos, aircraft, submarines, and mobile ground units) is activated from these bases in the case of a missing link with the strategic missile control centre. Perimeter checks this link all the time, but it can act autonomously if needed. Another example is the Russian fully automated nuclear submarine Poseidon, which can also autonomously launch a nuclear attack.[73]

3.4. Cyber Warfare and Cyber Security Applications

AI systems can also be used both offensively and defensively in cyberspace. On the offensive side, AI-generated cyberattacks are conducted with greater speed, accuracy, and anonymity. Cyberattacks have also been used to spread AI-generated malware and fake news.[74] AI can automate many aspects of cyberattacks, making them more effective and difficult to detect. The transformative nature of this threat suggests that AI-powered software can learn and adapt in real time. Even a chatbot

71 Ibid., p. 5.
72 Ibid., p. 4.
73 Luberisse, 2023a, pp. 21–23.
74 Ibid., p. 12.

ChatGPT, an interactive language model, trained constantly by its public users, can be used as a weapon by cybercriminals for many purposes, such as crafting convincing phishing emails and other polymorphic malware (mass social engineering), automated attacks, and distributed spamming. Thiele stressed that developments are moving towards AI-driven cyber attacks, in which malware has the ability to self-propagate via a series of autonomous decisions and intelligently tailor itself to the parameters of the infected system.[75] Gatopoulus reminds us that one of the early examples of AI weapons is likely Stuxnet,– software that could hide itself, cover up its tracks, search for a particular piece of code to attack, and damage Iranian centrifuges. However, the present capabilities of the tools are likely to be much higher.[76] Another application of AI is in weaponising information by producing false narratives and false videos – known as deepfakes.[77] Deepfake technology uses deep learning to alter images, videos, and audio content or create them from scratch. Deepfake is presently used predominantly in the pornographic industry (96 % of all deepfake products), and the difference between reality and produced output is increasingly blurred. Portraying political leaders in unreal situations will likely impact political certainty and create crises. Increasingly, we will see new developments in counter-deepfake technology.[78]

On the defensive side, AI algorithms can analyse a large amount of data to identify potential threats, vulnerabilities, patterns, and anomalies in network traffic, providing early warnings of potential cyberattacks. According to Thiele, autonomous cyber AI can detect what is normal in networks and thus identify anomalies and unknown threats at an early stage and react to them autonomously before damage occurs. In the future, algorithms will fight algorithms. The autonomous systems with the best AI will win.[79] Armed forces can use AI software that employs machine learning to identify and predict threats before they can affect networks and neutralise threats when needed. These systems (e.g. Cylance) are efficient at detecting and stopping tens of thousands of events per day which have not been detected by anti-virus systems.[80] Cylance, a software likely used by the CIA, seems able to identify and neutralise dangerous emails laced with malware. Its AI learning model was trained using millions of emails, some containing malware and phishing scams. The trained algorithm can scan incoming mail and assess related threats.[81] AI can be used to detect synthetic activities such as smart bots and deep fakes.[82]

Interestingly, defending the U.S. position against AI-capable adversaries operating at machine speeds requires the employment of AI; otherwise, it will lead to

75 Thiele, 2021f, p. 201.
76 Gatopoulos, 2021, p. 10.
77 See: Thiele, 2021b, p. 78.
78 Rickli and Mantellassi, 2023, p. 22.
79 Thiele, 2021f, p. 201.
80 Roth, 2019a.
81 Roth, 2019c.
82 Nurkin, 2023, p. 51.

disasters. Human operators will not be able to keep up with or defend against AI-enabled cyber or disinformation attacks, drone swarms or missile attacks without the assistance of AI-enabled machines. The plan is to leverage AI-enabled cyber defences against AI-enabled cyberattacks.[83]

3.5. AI-enabled Logistics

In addition to the aforementioned logistical applications, we should also stress the capability of AI to allow for more efficient, data-backed logistics and the maintenance of military equipment. These systems can generate alerts when, for example, the ammunition is reduced below a certain threshold (e.g. 15 %) or visualise damage reports in 3D to help maintenance engineers to diagnose and make decisions (reducing the time needed for decision-making).[84] For example, the U.S. Armed Forces already use predictive logistics with intelligent calculation of repair and maintenance tasks. Several aircraft, such as the F-22 and F-35, are equipped with logistical internal sensors and software.[85]

3.6. AI-based Training and Exercises

AI can make virtual and real exercises more realistic and demanding so that personnel are better prepared for complex operations. Thus, AI can significantly improve the realism of tactical training.[86] Additionally, real-world and virtual world training will be developed (e.g. dogfights between piloted and virtual aircraft, leading to cost reductions by creating and equipping the so-called red teams).[87] Intelligent algorithms can play the role of adversaries or populations to produce fine-grained analyses, develop new operational concepts and tactics, predict the best ways to use new technologies, and integrate them into existing systems. Virtual reality will considerably improve the realism of tactical training.[88]

AI can also be used to create and constantly update the personalised curricula of military trainees depending on their learning styles, and for objective promotion and posting of cadres.[89]

Another training-related issue is the training of AI algorithms. Limited datasets are not suitable for training algorithms, as large amounts of data are required to train them. Additionally, access to such data may be counterproductive if the data have not been effectively curated or managed.[90] Over time, AI systems will mature,

83 Schmidt et al., 2021, p. 9.
84 Roth, 2019a.
85 Mashur, 2019, p. 4.
86 Roth, 2019, cited in Thiele, 2021e, p. 189.
87 Nurkin, 2023, p. 46.
88 Mashur, 2019, p. 3.
89 Ibid., p. 3.
90 Nurkin, 2023, p. 54.

and their success rate will improve. The more information these systems have, the more accurate they will be in terms of perception, assessment, and actions. This will help to overcome the challenge of trust among human operators of AI systems.[91] An example is the AI training of drones in a structured learning process using a learning algorithm. AI supports the preprocessing of the sensor data and flight-control systems. The principles of learning are as follows (using a case of city traffic, but equally applicable to drones): researchers feed AI with thousands of videos of car and bicycle drivers behaving exemplarily in traffic. Over time, the algorithm derives rules of behaviour – it understands how to follow roads without getting into oncoming traffic and how to stop in time before obstacles, such as pedestrians, vehicles, and roadworks. It learns to solve complex tasks by using numerous training examples.[92]

4. Identification and Analysis of a Broad Spectrum of Concerns and Challenges Related to the Use of Artificial Intelligence by Armed Forces

In addition to the numerous benefits of using AI, there is also a broad spectrum of concerns and challenges. All these concerns reflect the need for, or difficulty in any potential regulation of the use of AI. These concerns span technical, bureaucratic implementation, and ethical, legal, and human rights to geopolitical and power-related concerns. We will focus in this chapter on the challenge of complex interconnections between AI and other non-AI disruptive technologies and on several geopolitical and strategic challenges.

4.1. The Challenge of Interconnected AI and non-AI Disruptive Technologies

Considering the regulation of AI, we forget that non-AI disruptive technologies strongly affect the use of AI in all dimensions, including the military. The same is true in the other direction – the future RMA V will be based on several other (non-AI) disruptive technologies; however, AI will penetrate them all and enable them to improve their output and even serve to help mitigate related security risks.[93] AI and machine learning will not individually impact the future military capability but will converge with other advanced technologies to create disruptive and potentially

91 Gatopoulos, 2021, p. 6.
92 Thiele, 2021f, pp. 198–199.
93 See: Thiele, 2021b, pp. 72–115.

transformative capabilities.[94] Below, we identify and briefly present other technologies that need to be regulated together with AI (mostly based on Nurkin).

- Fifth-Generation Technology – the 5G standard for cellular networks is a new technology that enables the use of real time computer-intensive technologies, such as AI, quantum computing, facial recognition software and cryptography, in mobile devices across the network. The increased use of the cloud has led to a corresponding increase in the demand for better connectivity, in the form of 5G, to speed up data transmission.[95]
- Additive manufacturing (3-D printing) refers to creating 3-dimensional solid objects of practically any shape using digital models. Armed forces will benefit from the possibility of quickly manufacturing parts, equipment, or weapons on the field in a highly decentralised logistics chain, reducing the logistical footprint, and improving repair time. AI will enable point-of-use printing of critical supplies, such as un-crewed systems, weapons, and spare parts. This has already been demonstrated by certain militaries during the COVID-19 crisis (e.g. printing protective equipment and ventilators).[96]
- Autonomous systems that include unmanned aircraft systems, robots, ships, vehicles, and other appliances will benefit from AI in terms of improving their autonomy (the ability to respond to uncertain situations independently, more sophisticated decision-making, and increasingly complex man-machine teaming). It can be assumed that manned systems will be escorted by swarms of unmanned systems (e.g. drones), which will be led by the manned system to some extent. Human-machine Teaming will become a critical capability in future military operations. There will also be virtual autonomous systems, such as malware with the ability to self-propagate via a series of autonomous decisions, intelligently tailoring itself to the parameters of infected systems.
- Biotechnology, as an innovation based on biology, will be significantly improved by increased data processing and AI (e.g. projects for improving war fighter survivability on the battlefield, introducing a wide range of materials, new sensors, and even possibilities for fast and large-scale production of natural infectious pathogens, their genetic modification for good and bad). AI will enable the development of new microbes with novel properties that do not exist in nature, as well as next-generation living camouflage and other novel organisms and materials.[97] Additionally, AI will enter neuroscience by directly enhancing the human brain for two-way data transfer, improving human-to-human and human-to-unmanned and autonomous machine communications, and data transfer (human-machine teaming). The idea of "cyber

94 Nurkin, 2023, p. 38.
95 Nurkin, 2023, p. 41.
96 Nurkin, 2023, p. 47.
97 Ibid., p. 48.

soldiers" stems from this direction, but is not realisable in the immediate future.[98]

- Cloud connectivity and secure storage of data are a priority in the armed forces as more data and applications become available through the Internet of Things (IoT).[99] Cloud computing outsources the limited IT capacity of a given local user to provide professional storage for large amounts of data hosted in several different places. According to Pomerlau, 'data is the ammunition of the future fight'.[100] The military needs the cloud to improve efficiency (e.g. network-centric warfare, improved exploitation of intelligence, and real time information sharing) while simultaneously reducing costs. AI and machine learning require cloud services.
- Communications that support military Command and Control (C2) systems or the modern derivative C4ISR (Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance) must be fast, ubiquitous, reliable, and secure. Facing threats on a multi-domain battlefield requires every soldier, platform, or weapon system to be digitally linked to a network. AI, machine learning, and cloud computing will be critical for enhancing and accelerating decision-making capabilities and paving the way towards the Internet of Battlefield Things (IoBT). The results will be intelligent networks of wireless devices with forming, dispersing, and self-healing capacities (based on adequate algorithms).
- Cyber capabilities involve using information and communication technology, including the Internet, for defensive and offensive purposes. Cyber threats come from individuals, criminal or terrorist groups, NGOs, states, or international actors aiming to exploit the vulnerabilities of the existing infrastructure. Offensive cyber operations can be used for reconnaissance or surveillance, intrusion, confusion, damage or sabotage, information overload (denial-of-service attacks), secret data theft, manipulation of information, propaganda or disinformation campaigns. AI is increasingly being used to develop malware against which it is impossible to protect, and develop high-end monitoring, detection and reconfiguration tools. AI will also increase the challenge of attribution. An additional worrying application is the micro-targeting of individuals, where social media information is used to create target profiles and then micro-drones are sent to spy on or neutralise them.
- Distributed ledger technology for protecting data access (data security) and cryptographic protection can be improved by integrating blockchain technology and AI. The goal is to create impenetrable blockchain security protocols.

98 Ibid., p. 45.
99 Ibid., p. 41.
100 Pomerlau, 2020, cited in Thiele, 2021b, p. 84.

- IoBT is the military version of the IoT, where an increasing amount of military equipment (sensors, weapons, ships, aircraft, vehicles, etc.) and soldiers themselves are integrated into the network. This can improve planning and logistical tasks, detection of friends or enemies, access-control to military facilities, surveillance of areas, and even, for the first time, to generate a truly comprehensive real time multi-domain operational picture and situational awareness. AI combined with IoT can significantly increase the impact of hybrid attacks. Special use of this will be in cognitive hacking, where the characteristics of individuals or groups will be sensed, analysed, and used against them.[101]
- Microelectronic chips are integrated electrical circuits that perform increasingly complex calculations in increasingly smaller spaces, thereby increasing the power of the hardware. AI applications will enable improvements in data storage, flexibility, and processing. Chip production is a major target for securing independent access to high-performance electronics.
- Quantum science harnesses the properties of quantum physics to enable new capabilities in computing, communication, cryptography, navigation, and sensing by adding sensitivity, accuracy, speed, and ease of use. This has wide applicability in the armed forces, and AI can enable navigation in closed spaces without global navigation satellite systems, improve encryption, break into encrypted messages, and process volumes of data.
- A wide range of omnipresent sensors will make the world into one large. There will be few places left to hide. Coupled with AI analysis, data from different sensors can be combined, fused, processed, and utilised.
- Extended reality (XR) is an umbrella term for virtual reality (reproducing reality in virtual space – VR), mixed reality (virtual reality enriched with selected virtual information MR) that includes augmented reality (AR), which refers to augmenting the real-world picture with the help of AR (e.g. projected by the head-up displays). This is enabled by immersive technologies that can couple real and virtual data and, for example, improve the tactical movement of soldiers through difficult terrains, explore operational areas or reported threats, and train military personnel. Training applications based on digital reproductions of targets are particularly convincing.
- Hypersonic weapons (glide vehicles and cruise missiles) fly at extreme speeds of Mach 5 and can be used effectively on targets or for missile defence systems. They are manoeuvrable, can avoid enemy air defence, can be armed with a nuclear head, and can be used in the pre-emptive destruction of the enemy's strategic weapons.

101 The push to connect data from all platforms, systems, people and physical infrastructure is leading to an explosion in the production of information available to the defence and security sectors, including high resolution imagery, video and biodata, see: Nurkin, 2023, p. 41.

- Directed energy (high-energy lasers and high-power microwaves) can be used effectively in defensive or offensive operations.
- Nanomaterials are phenomenally small and outperform conventional materials. They can be used in intelligent textiles (clothing with greater tolerance for temperature variations and enhanced protection against bullets), bio-and chemical agents, for sealing fabric pores, improving armour protection, improving penetration of ammunition, and improving stealth capability.
- Digital engineering will also benefit from AI. For example, a new generation of fighter aircraft can be designed using AI-enabled computer models, allowing engineers to test millions of possible designs in the virtual world before building a physical aircraft into an optimised design. This also reduces the cost and time required for the development.[102]

4.2. Geopolitical and Strategic Challenges

Geopolitical logic has been increasingly applied in the development and application of AI. AI is a new tool and represents an irresistible opportunity for states, corporations, and individuals to project power.

Geopolitics has internal and external aspects.

Internal geopolitical aspects: Bremmer and Suleyman warn that AI will unlike previous technological waves initiate a seismic shift in the structure and balance of global power, as it threatens the status of nation states as the world's primary geopolitical actors. AI creators will become geopolitical actors because they are entering an area generally reserved for nation states. AI will empower those who wield it to survey, deceive and control populations, or collect personal data in both democracies and repressive regimes. Only a handful of large and specialised companies currently control aspects of AI development, and they will also jealously guard their advantage for the foreseeable future. Countries are likely to support their own national AI champions, and the AI revolution will take place outside the control of governments. This means that the direction of AI development will largely be determined by decisions taken by private businesses, regardless of the actions of policymakers in Brussels and Washington.[103]

External geopolitical aspects: Bremmer and Suleyman stressed that AI will be the focus of intensive geopolitical competition. Competition for AI supremacy will be a strategic objective of every government with the resources to compete. Two key players, the U.S. and China, see AI development as a zero-sum game that will give the winner a decisive strategic edge in the future.[104] Nations and organisations that are best positioned to anticipate and exploit technological opportunities will likely have a decisive advantage in future crises and conflicts. AI will also be the

102 Nurkin, 2023, pp. 41–51.
103 Bremmer and Suleyman, 2023, pp. 2–9.
104 Ibid., pp. 7–8.

linchpin for achieving military superiority through the use of data, transforming it into relevant information, usable knowledge and finally into decision advantage.[105] All systems will be used in the pursuit of power. Schmidt et al. fear that all AI tools will be the weapons of first resort in future conflicts.[106] The ability to innovate in this field has become synonymous with international influence and national power – generating economic competitiveness, political legitimacy, military power and even internal security.[107]

A trade and technological war between the U.S. and China has already begun. In 2022, the U.S. introduced sanctions on the export of chips and related production equipment to China. In July 2023, China prohibited the export of Gallium and Germanium to unfriendly states.[108] The U.S. President Biden, by the Presidential Directive in August 2023, adopted another decision on the limitation of U.S. investments in Chinese companies in the fields of AI systems, semiconductors, and quantum technologies. This was motivated by as concern for national security risks. Officials in Beijing responded critically by saying that this would damage U.S. and Chinese companies. The EU has not followed the U.S. example on this yet, but the president of the EC (von Leyen) introduced in her speech in March 2023 a new policy of de-risking, that is, limiting transfers of capital, expertise, and knowledge of European companies to strengthen the military and intelligence capabilities of system rivals. Dual-use technologies will be at the heart of further limitations imposed by the EU.[109] The U.S. is doing everything to stop Chinese access to certain technological segments based on its experience with Chinese copying of technologies which has brought China to its current technological level. The Australian Institute for Strategic Policy has assessed that China has already surpassed the U.S. in 37 out of 44 key technologies in the fields of defence, space, energy, and biotechnology.[110]

Luberisse wrote a book on Geopolitics of AI, its impacts international stability and how it raises the risk of accidental use. The use of AI raises several security risks, one of which is the geopolitical risk of a power struggle between great powers, with implications for the balance of global power. Accordingly, AI intersects with geopolitics in several ways.

- Through use in military applications, leading to concerns about effects.
- Through use in intelligence and espionage, leading to the same concerns.
- Through its impact on the global economic landscape, for example, by automating many jobs, improving the efficiency of various industries, and affecting the global distribution of wealth and power.

105 Thiele, 2021b, pp. 59, 77.
106 Schmidt et al., 2021, cited in Thiele, 2021b, p. 76.
107 Raska and Bitzinger, 2023, p. 2.
108 Baković, 2023a p. 6; 2023b, p. 6.
109 Žerjavič, 2023, p. 5; Baković, 2023b, p. 6.
110 Baković, 2023a, p. 6.

– Through its impact on human rights and civil liberties in the sense that AI could be used to violate them, as suggested by the Chinese use of AI to monitor and suppress its own citizens.[111]

The AI power struggle refers to ongoing competition among great powers to develop and deploy advanced AI technologies in their military and intelligence operations. This competition is driven by the potential for AI to fundamentally change the balance of power in the international system. Great powers such as the U.S., China, Russia, and several European countries are actively investing in AI to gain an advantage in this ongoing power struggle. These investments include funding for AI research and development, deployment of AI in military and intelligence operations, and the development of AI-powered weapons and surveillance systems.[112] In addition, the frontrunners of the global revolution in military affairs, the U.S. and China, are engaged in a race to adopt AI and other emerging and disruptive technologies.[113] Other authors believe that the U.S., Russia, and China have entered into a modern space race-style competition to develop and harness AI technologies.[114]

However, one important aspect of AI proliferation must be considered. AI technology will proliferate horizontally among states and vertically among non-state actors, and even individuals. This is a completely different pattern of proliferation from that of nuclear technology.[115] Luberisse stressed that the rise of AI-empowered states and non-state actors is inevitable and will create new forms of power asymmetry. Such states will be those that invested heavily in AI for military, intelligence, and surveillance operations who will play a major role in the future of geopolitics, and are likely to be more influential in international affairs. Non-state actors will enhance their ability to evade detection, conduct cyberattacks, and develop new weapons. These situations will create new challenges and opportunities. The major challenge will be the risk of an arms race in the development of AI technologies in the military and intelligence fields, which can lead to a destabilising cycle of competition and escalation. The challenge will also be to address the potential for autonomous weapons to be used in ways that violate international law and human rights. The main opportunity will be to improve collaboration between states and international organisations in developing these new technologies, enhance intelligence gathering, improve cybersecurity, and support peacekeeping and humanitarian operations.[116]

The desire to design and build new AI weapons that are expected to tip the balance in future conflicts has actually already triggered an arms race between the U.S. and its competitors, Russia and China. The application of AI is asymmetric, meaning that a small country can develop effective AI software without the need to research,

111 Luberisse, 2023a, pp. 5–6.
112 Ibid., p. 9.
113 Soare, 2023, p. 81.
114 Roth, 2019c.
115 Rickli and Mantellassi, 2023, p. 27.
116 Luberisse, 2023a, p. 15.

develop, or test new weapons systems. AI is a powerful way to leapfrog over the competition.[117] AI could potentially improve the speed and accuracy of everything in the military, which drives the acceleration of research and development of AI products. For the U.S., AI offers a new way to sustain its military superiority while potentially reducing costs and risk to U.S. soldiers. For Russia and China, AI offers the ability to disrupt U.S. military superiority. National competition in AI leadership is as much or more an issue of economic competition and leadership than anything else. Militaries will fear being left behind by the capacities of other actors.[118]

Incentives to research AI are not simply a matter of competitive pressure from other militaries. For democracies, autonomous systems offer the potential to achieve tasks at lower cost and risk to human personnel. For autocracies, AI systems allows reduction of their reliance on people, allowing them to operate using a smaller, more loyal, part of the population.[119] Another aspect of the geopolitical perspective is that AI could negatively impact the strategic stability between the nuclear superpowers by degrading the edge provided by supposedly invisible platforms, such as nuclear submarines and stealth aircraft.[120]

AI development and implementation in modern armed forces will typically lead to distrust among states with delicate geostrategic situations and a lack of information on the opponent's capabilities. Horrowitz stressed that a state's AI-related armament capabilities would be almost impossible to measure accurately by other states. Assessing the depth of automation, the quality of the code, the efficiency of autonomous weapons and their capabilities will be difficult. This uncertainty will lead states to overestimate other states' capabilities.[121]

A large part of the AI race is driven by the fear of being surpassed by competitors. For example, Haas stressed that the Western lead in military technology is dwindling.[122] It appears that Russia and China are advancing faster in AI battlefield technology compared to the armed forces in NATO and EU. Russia is focusing on AI applications on hybrid influencing and information warfare, and has also started equipping soldiers with information management tools to achieve information dominance in military operations.[123] Additionally, Russia is integrating AI in a remarkable range of weapons, from smaller firearms to the Armata T-15 tank, and its Tactical Missiles Corporation is working on AI-guided missile techniques.[124] Iran's focus on AI research and development has been the integration of AI with low-cost technologies such as drones and swarming techniques.[125] Another concern is the relatively

117 Gatopoulos, 2021, p. 11.
118 Horowitz, 2018, pp. 2, 7.
119 Ibid., p. 4.
120 Mashur, 2019, p. 3.
121 Horrowitz, 2018, cited in Rickli and Mantellassi, 2023, p. 25.
122 Haas in Thiele, 2021a, p. 65.
123 Everden, 2021, cited in Thiele, 2021e, p. 190.
124 Horowitz et al. 2018, p. 17, cited in Thiele, 2021e, p. 190.
125 Rubin in Thiele, 2021e, p. 190.

easy threat of proliferation of AI. Egel stressed that since AI-capable weapons are relatively easy and inexpensive to obtain, they are also accessible to non-state actors and proxies. Some states could even deliberately provide such actors with these capabilities, as has happened in the past.[126] Thiele concluded that AI technologies would sooner or later be available to any opponent.[127]

Russian President Putin said in 2017 that the nation with the leading edge in AI would be able to rule the world.[128] In the same year, Russia's Military Industrial Committee approved the integration of AI into 30 percent of its armed forces by 2030. However, current realities do not reflect this, as progress is patchy. The Uran-9 unmanned combat vehicles performed poorly on the urban battlefields of Syria in 2018, often not reacting to their surroundings or able to detect potential targets. Despite these setbacks, it was introduced into the Russian military in 2019. China has clearly stated that its major research and development focus is to win using intelligent(ised) warfare. The current research areas include AI-enabled radar, robotic ships, smarter cruise, and hypersonic missiles. Russia and China are no longer looking to achieve parity with U.S. in the field of AI, they are looking to surpass it by investing in research. For them, doctrine is also key because it is important to integrate AI into future war plans.[129]

The U.S. believes that AI is a world-altering technology and is likely to be the most powerful tool in generations for expanding knowledge, increasing prosperity, and enriching human experience. AI will also be a source of enormous power for the companies and countries that embrace it. However, AI is increasing the U.S.'s vulnerability, as its technological predominance (achieved after WW II) is under threat for the first time. China possesses the might, talent, and ambition to surpass the U.S. as the world's leader in AI in the next decade, if current trends do not change.[130] Director of the U.S. AI Center stated that we are going to be shocked by the speed, chaos and bloodiness of future wars, when it will be algorithm against algorithm.[131] The U.S. established the National Security Commission on Artificial Intelligence, which produced a report in 2021 containing a strategy to defend against AI threats, responsibly employ AI for national security, and win the broader technology competition. The council believes that AI systems will be used to pursue power, and fears that AI tools will become weapons of first resort in future conflicts. AI will not remain in the domain of superpowers, but because of its dual-use and open source nature, it will extend to state adversaries, criminals, and terrorists. The Commission also believes that the U.S. will not be able to defend itself against AI-enabled threats without ubiquitous AI capabilities and new warfighting paradigms. They point out that the U.S. government is far from being AI-ready and suggested that by 2025, the

126 Egel et al., 2019, cited in Thiele, 2021b, p. 77.
127 Thiele, 2021e, p. 190.
128 See Mashur, 2019, p. 1.
129 Gatopoulos, 2021, pp. 11–12.
130 Schmidt et al., 2021, pp. 7, 14.
131 Rickli and Mantellassi, 2023, p. 20.

DOD and Intelligence Community must be AI-ready.[132] Accordingly, the U.S. must embrace global AI competition or AI-accelerated competition (which is part of a wider global technology competition) and must win it. China's plans, resources, and programmes concern the U.S. The U.S. should take seriously its ambition to surpass itself as the world's AI leader within a decade.[133] The U.S. National Security Commission also declared China's advancement in AI a major threat to American dominance in the AI industry. China is described as a U.S. peer and AI leader in some areas. In this regard, China will counter U.S. military superiority by intelligently redesigning war by placing greater emphasis on new logistics, procurement, training, and warfare methods.[134]

Part of the external AI geopolitical struggle concerns values. AI competition is also a competition about values. The U.S. is concerned about China's use of AI as a tool for repression and surveillance at home and abroad. Accordingly, AI should reinforce democracy rather than erode it. The future of AI should be democratic; the U.S. believes AI must be developed based on its values and must work with democracies and the private sector to build privacy-protecting standards into AI technologies and advance democratic norms to guide AI use so that democracies can responsibly use AI for national security purposes. The U.S. is also worried that the majority of cutting-edge chips are produced in a single plant separated by just 110 miles of water from its principal strategic competitor, China.[135] China has invested heavily in AI with a special focus on surveillance systems to enhance its ability to monitor and control its population. The deployment of AI-powered cameras and facial recognition systems across the country has raised significant concerns about privacy and human rights, and has fuelled debates about the appropriate use of AI. In 2017, China released its AI Development Plan and its Academy of Military Sciences was tasked with leveraging warfighting theory and doctrine to capitalise on disruptive technologies in the future "intelligentised warfare".[136]

4.2.1. The Situation in Europe

By contrast, the European public debate has focused almost entirely on the ethical and legal challenges AI presents. This has created a public ethical filter through which all European military AI projects are scrutinised, resulting in lower investment in AI in Europe than in the aforementioned states. Europe has found itself at a crossroads in the adoption of military AI: 'either European countries overcome their reluctance and risk aversion to accelerate investment and rapid integration of AI technologies in defence over the mid-term, or they risk becoming less strategically and militarily

132 Schmidt et al., 2021, pp. 1–2.
133 Ibid., pp. 2, 8.
134 Luberisse, 2023a, pp. 12–13.
135 Schmidt et al., 2021, pp. 2–6.
136 Luberisse, 2023a, pp. 10–11.

competitive'.[137] The European approach to AI is fragmented and uneven across countries, and has been de-linked from threat perception. In Soare's view, four variables explain this situation:

1. There is a robust European preference for national AI adoption models in which these technologies are used to incrementally optimise legacy platforms and overcome persistent capability gaps. National approaches are incoherent, and their ambitions vary: while some countries place great emphasis on developing military AI (France and the UK developed AI defence strategies; Netherlands, Finland, Spain, Italy, Estonia, Denmark, and Turkey developed AI adoption plans and policies of varying scope), others barely mention it (e.g. the German MoD Paper on the future of Bundeswehr from 2021 barely mentions emerging and disruptive technologies). This leads to support for more national AI champions instead of focusing on intra-EU technological cooperation in AI development.[138]
2. National defence establishments and regional organisations such as the EU and NATO struggle to adopt a more visible role in shaping technological progress dominated by commercial, market forces, and academia. All European countries suffer from the problem of seeing AI more as an incremental enabler of optimising military power instead of a declarative (by them as well) disruptive defence technology.[139]
3. European states underuse regional institutional accelerators of military AI adoption, such as the EU and NATO. The EU adopted the Strategic Compass in 2022, setting a goal to become a more assertive security and defence actor by enabling more robust, rapid, and decisive action, including for the resilience of the union. Accordingly, the EU plans to use AI to improve military mobility within and beyond the EU and make intensive use of new technologies, notably quantum computing, AI and big data and advanced propulsion, to achieve comparative advantages in the cyber domain, including in terms of cyber responsive operations and information superiority, boosting efforts at national and EU levels to be better prepared for the future battlefield.[140] In its *Strategic Concept* from 2022, NATO emphasises the importance of investing in technological innovation, which promises to enhance our individual and collective resilience and technological edge to fulfil the alliance's core tasks. This acknowledges that emerging and disruptive technologies bring both opportunities and risks, that they are altering the character of conflict, acquiring greater strategic importance, and becoming key arenas of global competition, and that technological primacy increasingly results in success on the battlefield. It promises to promote innovation and increase investments in

137 Soare, 2023, p. 80.
138 Soare, 2023, pp. 84, 92.
139 Soare, 2023, p. 91.
140 *A Strategic Compass for Security and Defence*, 2022, pp. 20, 32, 34.

emerging and disruptive technologies to retain interoperability and the EU's military edge.[141] NATO adopted its Artificial Intelligence Strategy in 2021 to provide a foundation for NATO and its allies to lead by example and encourage the responsible development and use of AI, accelerate and mainstream AI adoption in capability development and delivery, enhance interoperability within the alliance, protect and monitor NATO's AI technologies and ability to innovate, define principles of responsible use, and identify and safeguard against threats from the malicious use of AI by state and non-state actors.[142] NATO enables several AI projects within its structures (ACT, for example). However, there is no evidence that these technologies have transitioned to actual procurement.[143]

4. According to Soare, European states 'exhibit self-imposed ethical and legal restraints, bordering on cultural-technological conservatism, which inhibits an ambitious European agenda on adopting military AI'. European AI debates are dominated by ethical and legal concerns over the deployment of autonomous weapon systems, policy efforts towards trustworthy and democratic AI, and calls for comprehensive arms control of emerging technologies. This inclination toward European cultural norms will have strategic consequences.[144]

Collectively, these variables act as obstacles to effective European collaborative AI-enabled defence innovation. Such a fragmented approach also presents a real danger that creating a coherent normative and operational European governance framework for military AI in the 2020s will not be achieved. AI adoption efforts will be slower, capabilities will be fragmented and less interoperable, and EU and NATO institutional accelerators will be underused.[145]

Therefore, European states face several adoption challenges. First, the current level of AI investment lags behind that of China and the U.S.. The second is that AI investments are very asymmetric, and the third is that, the European Defence Fund and other mechanisms take too long between project proposal submission and acceptance. Third, defence officials lack the skills required to implement current AI projects. Fourth, leading powers are reluctant to participate in collaborative defence AI projects or to transfer sensitive AI technologies to other less tech-savvy European allies. This reflects a lack of trust and sensitivity to data sharing, and different funding opportunities.[146]

Accordingly, the EU Council and Parliament managed to strike a deal on the substance of the new AI Act in December 2023. This will represent the first legal act providing regulation for AI in the world, likely setting a global standard for AI

141 NATO, 2022, p. 1 et seq.
142 *Summary of the NATO Artificial Intelligence Strategy*, 2021.
143 Soare, 2023, p. 99.
144 Ibid., pp. 81–84.
145 Ibid., p. 81.
146 Ibid., pp. 85–89.

regulation and related human-centric approaches to AI. The aim of this document is to create a balance between boosting innovation and the uptake of AI across the EU while fully respecting fundamental citizens' rights. The EU fears that AI systems may jeopardise fundamental rights such as the right to non-discrimination, freedom of expression, human dignity, personal data protection, and privacy. The document will define AI (although the definitions used have been widely discussed and problematised), create an EU database for registering high-risk AI systems, create AI testing sandboxes, establish a governance framework based on EU and national AI regulatory entities, and limit the use of AI products using a risk-based approach.

The major caveat of the use of the AI Act is that

> regulation does not apply to areas outside the scope of EU law and should not, in any case, affect member states competences in national security or any entity entrusted with tasks in this area. Furthermore, the AI Act will not apply to systems which are used exclusively for military and defence purposes.[147]

Additionally the draft regulation will also not apply to public authorities in a third country and international organisations.[148]

NATO also adopted its policy and strategy in the field of AI. Interestingly, NATO published only a summary of its strategy and not the entire document. In this strategy, NATO aims to use AI to support its three core tasks (collective defence, crisis management and cooperative security) in an interoperable way and in accordance with international law. Specifically, the strategy aims to:

5. Provide a foundation for NATO and Allies to lead by example and encourage the development and use of AI in a responsible manner for Allied defence and security purposes;
6. Accelerate and mainstream AI adoption in capability development and delivery, enhancing interoperability within the Alliance, including through proposals for AI Use Cases, new structures, and new programmes;
7. Protect and monitor „our" AI technologies and ability to innovate, addressing security policy considerations such as the operationalisation of our Principles of Responsible Use; and
8. Identify and safeguard against the threats from malicious use of AI by state and non-state actors.[149]

NATO's strategy also recognises the risk of interference in allied AI by other states and non-state actors. Therefore, NATO must strive to prevent AI from being

147 *Artificial Intelligence Act: Council and Parliament Strike a Deal on the First Rules for AI in the World*, 2023, p. 1.
148 *Artificial Intelligence Act*, 2023, p. 3.
149 *Summary of the NATO Artificial Intelligence Strategy*, 2021, p. 1.

used for interference, manipulation, and sabotage. Additionally, unfriendly actors may leverage disinformation to create public distrust of the military's use of AI.[150]

This strategy was criticised by some immediately after its publication. For example, critics stressed that it was not explained why only the summary of this strategy was made public; there is no detail on how NATO's AI systems will be protected against threats from malicious actors or use; that the strategy exclusively understands AI applications in terms of a zero sum arms race against rivals (China and Russia); that the principles for responsible use are almost the same as U.S. principles for the ethical use of AI; and that they were not adopted in an open consultation but are more based on opinions from a narrow range of experts, likely mostly from the U.S.. An opinion poll conducted by the Pew Research Centre in 2021 found that 68 % of experts in the field think that ethical principles will not be applied to most AI systems by 2030. Finally, the strategy does not mention AI-driven autonomous weapon systems, which is a very serious deficiency. Burt concludes that NATO states would, if they are serious about ensuring that mlitary use adheres to international and human rights laws, call for and engage in negotiations for a legally binding instrument on autonomous weapons systems.[151]

The stakes are well explained by the Slovenian State Secretary of the Ministry of Foreign Affairs just before the country took a non-permanent seat at the UN Security Council in 2024. He observed that, on the one hand, AI is in the hands of autocratic regimes, and on the other hand, we know that some companies in democracies have already used it to influence elections (e.g. Cambridge Analytica). He recapitulated also the perception of the Slovenian President that the latter is a threat to democracy.[152]

5. Conclusion and Identification of Several Areas Where Regulation Is Needed

We can confirm our hypothesis in this paper that the emergence of AI has introduced a new level of possibilities to improve military and defence capabilities (benefits) and, but has simultaneously resulted in a broad range of concerns, challenges and risks. The first part of the paper showed how AI is conceptually embedded in the new wave of the RMA. Already this debate suggests that building an AI regulatory system will be a difficult task. Enthusiasts in the AI debate are right that AI will bring big change in warfare, but deniers are also right that this change will be slower than we expect due to many implementation difficulties. Interestingly, the Ukrainian military is an example of the fast implementation of AI with interesting apps that improve situational awareness and targeting based on information from multiple

150 Ibid., p. 3.
151 Burt, 2021, pp. 1–4.
152 *Samuel Žbogar, interview*, Sobotna priloga, Delo, 7 October 2023.

sources. However, AI did not turn out to be a game-changer against Russia. The real picture will likely unfold according to the prediction of pragmatics who stress that AI will find in an evolutionary (not revolutionary) way to the battlefield, but it will not change the immutable nature of war. From the perspective of a new regulatory architecture, this means that some AI technology will be tested on the battlefield, and some will also be misused (e.g. for surveillance purposes) even before regulations are in place (as was the case with most other technologies in the past). In time there will be initial regulation in place, and after some time and some negative examples of AI use or misuse, a chance for stronger regulation will appear. This human tendency to build a regulative framework over means of violence is not a new path.

This paper presents and analyses a broad spectrum of possibilities for the present and future use of AI by armed forces and defence establishments. It also raises critical points where regulation needs to be applied in a future comprehensive regulation structure. The boost will be huge in the fields of intelligence, surveillance and multi-domain situational awareness. AI predictive analytics will be able to improve decision-making processes by increasing quality and speed. The key regulatory question for predictive analytics is whether the obtained data is legally collected. Another regulatory question is whether AI training models work with legally obtained data. It is known that AI needs large amounts of data, and such data ambitions need to be regulated. The subject of targeting by autonomous weapon systems is extremely sensitive. If AI is tasked only with target identification with a human will having the task of approving engagement, then the existing regulatory framework (international war and humanitarian law) should suffice. However, if these systems gain complete autonomy from their human masters, the existing regulatory framework must be updated by attributing the responsibility for machine actions to their human masters. Mini-, micro-, and nano-unmanned military autonomous systems are being developed in the aerial, surface, undersea, and ground domains, where they will take over tasks that were previously performed by humans. From a regulatory perspective, there is the same issue of connecting legal responsibility to actions between the platform and its owner. An additional question is how to regulate the operation of aerial drone swarms. Flight-control regulations will likely need to be analysed for the required changes. Regulators will have to develop clear principles and standards for regulating the human-machine teaming in military and other civilian fields at all three levels of autonomy, such as human-in-the-loop, human-on-the-loop, and human-out-of-the-loop. In the case of human-out-of-the-loop, the question arises whether AI independent (weapon/autonomous) and other systems require an independent legal subjectivity, just like human persons. A very special regulative case are AI autonomous nuclear weapon systems. The wrong use or misuse in this case could have disastrous consequences for humankind. Differentiating between defensive and offensive AI nuclear autonomous systems makes little sense. In this case, a recommended regulatory direction could be an adaptation of existing nuclear weapons regulations, such as NPT. Human-in and human-on-the-loop remains vital from the perspective of prevention of uncontrolled escalation of nuclear war.

Cyber warfare and cyber security are very different applications of AI. Regulating the use of AI in this field will be extremely difficult because regulation is already difficult without AI. AI-generated cyberattacks will be automated and conducted with greater speed, accuracy, and anonymity, and the automatic generation of disinformation and deepfake videos will create confusion. The regulation of this field is complex and partially ineffective. AI-enabled logistics is completely different, and it appears that no special precautionary regulations will be needed. AI logistics systems will simply continue to support the logistical process and comply with existing logistical regulations. In AI-based training and exercises, two aspects are relevant. Firstly, the use of AI in training raises the question of the interaction between AI and human trainees. This area will be very important for creating the right balance between the role of human-in/on or out of the loop. Furthermore, training of the AI itself is always based on big data and the typical regulative question here is about the algorithms access to data, the legality of data collection, protection of stored data, and access to the data collected by AI algorithms, etc.

This study identifies several strategic and geopolitical concerns regarding the development and use of AI systems. All the identified concerns also reflect the need for or difficulty in any potential regulation of the use of AI. The first concern is the challenge of complex interconnections between AI and other non-AI-disruptive technologies. AI has and will penetrate the technological fields of Fifth-Generation Technology (5G), additive manufacturing (3-D printing), autonomous systems, biotechnology, cloud connectivity and secure storage of data, communications that support military Command and Control (C2) systems or modern derivative C4ISR (Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance), cyber capabilities, Distributed Ledger Technology for protecting data access (data security) and its cryptographic protection, IoT, microelectronic chips, quantum science, omnipresent sensors, Extended reality (XR), hypersonic weapons, directed energy, nanomaterials, digital engineering, etc. The lesson here is that we will need not only AI technology regulation, but that regulations in all of these fields will have to be updated with an eye on the use of AI.

Several geopolitical and strategic challenges have been identified in this paper. Geopolitical logic has been applied to the development and application of AI because stakeholders see it as a source of power and a new tool for projecting power. Internal geopolitical prisms suggest that AI creators or companies will become geopolitical actors at the expense of nation states. The regulatory need here, is to limit the power of these companies in the development and use of AI. On the other hand, the external geopolitical prism suggests the intensification of geopolitical competition for AI supremacy among states will be helped by certain AI companies. AI has the potential to change the balance of power for nations, that is, to increase own power and reduce the power of the opponent. AI is perceived as a commodity and a weapon; therefore, there will be an AI arms race. This zero-sum struggle has the potential to create new wars on its own–for example, a war for control over AI technology. AI companies and their AI technologies could become the main targets in future armed conflicts.

The AI supremacy race will give rise to many interstate uncertainties about existing capabilities and intentions and will consequently create a lack of trust. This is not a new situation in the international system. As in the past, we will have to develop new confidence- and security-building measures (CSBM) in the AI field. In other words, existing CSBMs will have to be extended to the AI field and be incorporated into AI weapon platforms to adjust the thresholds of AI-supported weapons. The proliferation of AI among states and from states to non-state actors has become an issue, and some limitations will likely have to be imposed. AI proliferation is much easier than, for example, nuclear proliferation; however, certain lessons from nuclear proliferation limitations can also be applied in this field. An AI non-proliferation treaty (analogous to the classic NPT treaty to limit the spread of nuclear technology) could be discussed.

Internally, in each state, human rights and privacy concerns have emerged because of some states' intentions to use AI to monitor and control their populations. Such use of AI will have to be regulated from the perspective of privacy and human rights, and AI will have to be utilised according to democratic values.

There is no doubt that we need to create a comprehensive AI governance system at regional and global levels. The questions are around how to create it, around which key issues it should be created, how comprehensive it should be and how many actors should be included. These are quite demanding questions, and the dynamics of AI development and use suggest that policies and regulations are lagging. There is a widespread call for regulatory action. The G-7 launched the Hiroshima AI process to harmonise AI governance; the European Parliament passed the first draft of the EU AI Act, and the European Council and European Parliament agreed on the document, the UN General Secretary called for the establishment of a global AI regulatory watchdog. With so many regulatory initiatives, how to connect them into a multi-level cross-domain effective regulatory system will need to be explored, and all gaps in the system that could be exploited identified.

The AI governance system must be built around key risks, such as the unpredictability of autonomous systems with self-improving capabilities, the risk that AI algorithms could easily proliferate, and the dual-use nature of AI technology, where the same algorithms can be used for civilian or military purposes. Additionally, a comprehensive AI governance framework needs to also incorporate the military and defence industries. Companies and their laboratories and programmers should not be left out of the regulatory framework.

This new regulatory system needs to be created as we introduce AI into the armed forces, as including AI technology as a technical change will require additional organisational, structural, doctrinal, and operational changes. Armed forces personnel and civil professional and political structures will need to understand the need for comprehensive socio-technical change. When AI is completely integrated into the armed forces, the future battlefield will use a creative mix of RMA I to RMA V tools to pursue its objectives. This means that any new AI regulatory framework will have to be synchronised with and connected to existing regulatory frameworks.

References

Artificial Intelligence Act (2023) Briefing, EU Legislation in Progress, European Parliamentary Research Service, June 2023.

Artificial Intelligence Act: Council and Parliament Strike a Deal on the First Rules for AI in the World (2023) Council of the EU, Press Release 986/23, 9 December 2023. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/ (Accessed: 3 May 2024).

Baković, Z. (2023a) 'Čip za čip, sankcija za sankcijo' [Chip for chip, sanction for sanction], *Delo*, p. 6.

Baković, Z. (2023b) 'Bianko ček za znanstvene preboje' [Bianco cheque for scientific breakthroughs], *Delo*, 12 August 2023, p. 6.

Bremmer, I., Suleyman, M. (2023) 'The AI Power Paradox: Can States learn to Govern Artificial Intelligence – Before It's Too Late?', *Foreign Affairs*, 16 August 2023. [Online]. Available at: https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox (Accessed: 1 December 2023).

Burt, P. (2021) 'NATO's New AI Strategy: Lacking Substance and Lacking in Leadership', Briefing paper No. 88, NATO Watch, 8 November. [Online]. https://natowatch.org/sites/default/files/2021-11/briefing_88_nato_ai_strategy.pdf (Accessed: 22 October 2023).

Cooper, J.R. (1994) *Another View of the Revolution in Military Affairs*. Carlisle, United States: Strategic Studies Institute of the US Army War College (SSI). [Online]. Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/pub240.pdf (Accessed: 9 October 2013).

Copeland, B.J. (2023) 'Artificial Intelligence', *Encyclopaedia Britannica*, 14 September 2023. [Online]. Available at: https://www.britannica.com/technology/artificial-intelligence (Accessed: 17 August 2023).

Davis, N. (1996) 'An Information-Based Revolution in Military Affairs', *Strategic Review*, 24(1), pp. 43–53.

Dustin, J. (2016) *AI Security*. Fort Myers: Undine.

Gatopoulos, A. (2021) 'Project Force: AI and the Military – a Friend or Foe?', *Aljazeera*, 28 March 2021. [Online]. Available at: https://www.aljazeera.com/features/2021/3/28/friend-or-foe-artificial-intelligence-and-the-military (Accessed: 17 August 2023).

Horowitz, M.C. (2018) 'The Promise and Peril of Military Applications of Artificial Intelligence', *Bulletin of the Atomic Scientists*, 23 April 2018. [Online]. Available at: https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/ (Accessed: 17 August 2023).

Horowitz, M., Rosen, S. (2005) 'Evolution or Revolution?', *Journal of Strategic Studies,* 28(3), pp. 437–448; https://doi.org/10.1080/01402390500137317.

Hundley, R.O. (1999) *Past Revolutions, Future Transformations What Can the History of Revolutions in Military Affairs Tell Us about Transforming the U.S. Military?*. Santa Monica, California: Rand.

Jahankani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J. (eds.) (2020) *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*. Cham: Springer Nature.

Krause, M.E. (1997) 'Night Air Combat: A United States Military-Technical Revolution. A Research Paper presented to the Research Department Air Command and Staff College In Partial Fulfillment of the Graduation Requirements of ACSC', March. [Online]. Available at: http://www.fas.org/man/dod-101/sys/ac/docs/97-0604G.pdf (Accessed: 14 October 2013).

Lange, N. (2023) 'How to Beat Russia: What Armed Forces in NATO should Learn from Ukraine's Homeland Defense', *GLOBSEC*.

Levy, A., Uri, M. (1986) *Organisational Transformation: Approaches, Strategies, Theories*. New York: Praeger.

Luberisse, J. (2023a) *The Geopolitics of Artificial Intelligence: Strategic Implications of AI for Global Security*. Wroclaw: Fortis Novum Mundum.

Luberise, J. (2023b) *Algorithmic Warfare: The Rise of Autonomous Weapons*. Wroclaw: Fortis Novum Mundum.

MacGregor, K., Murray, W. (2001) 'Thinking about Revolutions' in MacGregor, K., Murray, W. (eds.) *The Dynamics of Military Revolution, 1300-2050*. Cambridge, UK; New York: Cambridge University Press, pp. 1–12.

Mashur, N. (2019) 'AI in Military Enabling Applications', *CSS Analyses in Security policy*, 2019/251, pp. 1–4. [Online]. Available at: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/367663/CSSAnalyse251-EN.pdf?sequence=2 (Accessed: 22 August 2023).

NATO (2022) 'NATO 2022 Strategic Concept', adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022. [Online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (Accessed: 1 July 2022).

Nurkin, T. (2023) 'AI and Technological Convergence: Catalysts for Abounding National Security Risks in the Post-COVID World' in Bitzinger, R.A., Raska, M. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. New York: Routledge, pp. 37–58; https://doi.org/10.4324/9781003218326-3.

Okechukwu, J. (2021) 'Weapons Powered by Artificial Intelligence Pose a Frontier Risk and Need to be Regulated', *World Economic Forum*, 23 June 2021. [Online]. Available at: https://www.weforum.org/agenda/2021/06/the-accelerating-development-of-weapons-powered-by-artificial-risk-is-a-risk-to-humanity.

Osinga, F. (2010) 'The Rise of Military Transformation' in Terriff, T., Osinga, F., Farrell, T. (eds.) *A Transformation Gap? American Innovations and European Military Change*. Stanford, CA.: Stanford University Press, pp. 14–34; https://doi.org/10.11126/stanford/9780804763776.003.0002.

Raska, M. (2011) 'The 'Five Waves' of RMA Theory; Processes, and Debate', *Pointer, Journal of the Singapore Armed Forces*, 36(3-4), pp. 1–12.

Raska, M., Bitzinger, R.A. (2023) 'Introduction: The AI Wave in Defence Innovation' in Raska, M., Bitzinger, R.A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. New York: Routledge, pp. 1–11; https://doi.org/10.4324/9781003218326-1.

Rickli, J.-M., Mantellassi, F. (2023) 'Artificial Intelligence in Warfare: Military Uses of AI and Their International Security Implications' in Raska, M., Bitzinger, R.A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. New York: Routledge, pp. 12–36; https://doi.org/10.4324/9781003218326-2.

Roth, M. (2019a) 'Artificial Intelligence in the Military – An Overview of Capabilities', *Emerj*, 22 February 2019. [Online]. Available at: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/ (Accessed: 7 September 2023).

Roth, M. (2019b) 'AI in Military Drones and UAVs – Current Applications', *Emerj*, 22 November 2019. [Online]. Available at: https://emerj.com/ai-sector-overviews/ai-drones-and-uavs-in-the-military-current-applications/ (Accessed: 7 September 2023).

Roth, M. (2019c) 'Artificial Intelligence at the CIA – Current Applications', *Emerj*, 22 November 2019. [Online]. Available at: https://emerj.com/ai-sector-overviews/artificial-intelligence-at-the-cia-current-applications/ (Accessed: 7 September 2023).

Roxborough, I. (2002) 'From Revolution to Transformation: The State of the Field', *Joint Force Quarterly*, 2002/32.

Samuel Žbogar, interview, Sobotna priloga, Delo, 7 October 2023.

Schmid, J. (2021) 'Introduction to Hybrid Warfare – A Framework for Comprehensive Analysis' in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 11–32; https://doi.org/10.1007/978-3-658-35109-0_2.

Schmidt, E. (Chair) et al. (2021) *Final Report*. Washington, D.C.: National Security Commission on Artificial Intelligence. [Online]. Available at: https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (Accessed: 2 September 2023).

Schuller, M. (2023) 'Human and Machine Learning', Paper presented at a conference NATO in the Nordics, August 30-31st 2023, Stockholm.

Sheehan, M. (2008) 'The Changing Character of War' in Baylis, J., Smith, S., Owens, P. (eds.) *The Globalization of World Politics*, 4th edn. New York: Oxford University Press.

Soare, S. (2023) 'European Military AI: Why Regional Approaches are Lagging Behind' in Raska, M., Bitzinger, R.A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. 1st edn. New York: Routledge, pp. 80–111; https://doi.org/10.4324/9781003218326-5.

A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security (2022) 7371/22, Council of the EU, 21 March 2022. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf (Accessed: 17 August 2022).

Summary of the NATO Artificial Intelligence Strategy (2021) Meeting of Defence Ministers, 22 October, Brussels. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_187617.htm (Accessed: 12 December 2022).

Thiele, R. (2021a) 'Technology as a Driver' in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 59–70; https://doi.org/10.1007/978-3-658-35109-0_4.

Thiele, R. (2021b) 'Nineteen Technologies in Focus' in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 71–124; https://doi.org/10.1007/978-3-658-35109-0_5.

Thiele, R. (2021c) 'Manoeuvring in the Hybrid Space' in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 125–154; https://doi.org/10.1007/978-3-658-35109-0_6.

Thiele, R. (2021d) 'Avenues to Adapt' in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 155–164; https://doi.org/10.1007/978-3-658-35109-0_7.

Thiele, R. (2021e) 'Annex 2 – Artificial Intelligence' in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 187–196.

Thiele, R. (2021f) 'Annex 3 – Autonomous Systems' in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 197–206.
Žerjavič, P. (2023) 'Geopolitika vse bolj narekuje gospodarski tempo' [Geopolitics increasingly dictates the economic pace], *Delo*, 17 August 2023, p. 5.

Chapter 9

Legal Aspects of Military and Defence Applications of Artificial Intelligence Within the European Union

Marko Jurić

Abstract

This chapter aims to map the primary legal instruments relevant to governing the use of artificial intelligence (AI) for military and defence purposes in Europe. The analysis indicates that, while there is no lack of regulation, the legal framework itself should not pose insurmountable obstacles for the industry and entities operating within the military and defence sectors. This issue is particularly evident in the regulation of lethal autonomous weapons systems (LAWS). There are no binding EU rules on this matter in the European Union (EU); however, some European institutions are advocating for reasonable safeguards to enhance human control and accountability.

The drafters of the EU AI Act have made concerted efforts to exempt the military, defence, and national security sectors from its scope. However, this does not mean that all AI-related activities in these domains will escape scrutiny by the Court of Justice of the European Union (CJEU). As existing case law demonstrates, the Court has in various areas under the primary competence of Member States, including matters of national defence. Therefore, it is possible that a similar approach may be applied in AI-related cases.

Finally, the most significant challenges in developing and using AI in the military and defence domains may arise from rules governing data usage. This chapter demonstrates that the current EU laws apply within the military and defence sectors. The possibilities for excluding their application appear narrower than in AI Act, particularly given the CJEU's established case law. Combined with the broad concept

Marko Jurić (2024) 'Legal Aspects of Military and Defence Applications of Artificial Intelligence Within the European Union'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 395–433. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_9

of personal data, it is easy conceivable that personal data protection rules could substantially impact the capacity of national defence and military entities to process certain data.

Keywords: Artificial intelligence, AI, military AI, defence AI, personal data, AI Act

1. Introduction

Artificial intelligence (AI) has been one of the most discussed issues in recent years. Everyone talks about it, and many want to use it for different purposes. As Rickli and Mantellassi write, it is 'the defining technology of this generation'.[1] The term AI appears everywhere, from office software to social networks. However, while one might be a bit sceptical about whether everything which passes for it nowadays is "true" AI, there seems to be little doubt that it will have a substantial impact on society.

Like in other spheres of human activity, the potential uses of AI in the military and defence sectors seem almost unlimited. But as in other sectors, there is also considerable debate on the use of AI for military and defence purposes. While autonomous drones and other lethal weapons systems that act without or with limited human control rightly occupy the top of the list of our concerns, there are many more areas where AI can make a meaningful impact. For instance, the U.S. Department of Defence considers that AI 'is expected to impact every corner of the Department, spanning operations, training, sustainment, force protection, recruiting, healthcare, and many others'.[2]

However, the expected impact of AI use might also involve many security, safety, ethical, and legal concerns associated with its use.[3] These issues are currently addressed mostly through various principles and codes of conduct, which provide guidelines for the responsible development of AI. However, this was true only in the initial phases. As noted by Anand and Deng, 'only a handful of states and intergovernmental organisations have publicly adopted principles, standards or ethical frameworks tailored to AI applications in the defence sector'.[4]

When we turn from the principles and codes of conduct, which at best can be seen as "soft law", towards binding legal norms, the situation is even more uncertain because AI legislation is yet to be developed. For instance, the EU's Artificial Intelligence Act, supposed to be the world's first comprehensive regulation of AI, was

1 Rickli and Mantellassi, 2023, p. 12.
2 U.S. Department of Defense, 2019, p. 5.
3 Anand and Deng, 2023, p. 6.
4 Ibid.

enacted during the writing of this chapter. In other jurisdictions, AI regulation is even less developed.

The purpose of this chapter is to analyse how the EU legal framework addresses the use of AI for military and defence purposes. As noted above, many parts of the legislation are currently still in development; therefore, in many aspects, this is a forward-looking and speculative analysis. There are several reasons for this observation.

First, there seems to be ambiguity regarding the possible uses of AI in the military. While it is almost universally acknowledged that the possibilities are immense, when we look at how militaries are planning to use AI, the situation is less clear. For instance, most NATO Member States do not currently have a dedicated military AI strategy. Only a few states (see below) have formalised their strategic thinking regarding military and defence AI. As noted in NATO's 2021 AI Strategy, military AI is still in early development.[5] Therefore, as AI technologies and their uses develop over time, regulatory issues will become increasingly emphasised.

Second, legal regulations for AI are also being developed daily. To illustrate this point, multiple versions of EU regulations regarding AI have been made public during the preparation of this contribution. In addition, with the growing understanding that AI can affect different sectors and activities, it is clear that some aspects of its use can be covered by existing rules. In the European context, this is most prevalent in the rules regulating the use of data.

2. AI in military and defence: what are the regulatory issues?

In this chapter, we seek to broadly map areas in which AI is already, or could be, used for military and defence purposes. This will be the basis for the analysis of the applicable legal framework in section 3. However, at the outset, we are already faced with problems of definition. To identify what might be the uses of AI in these sectors, we first have to define AI. The problem here is that there are many definitions of AI, and depending on the definition, the same system can be seen as either AI or not.[6]

For instance, the 2018 U.S. Department of Defense AI strategy broadly defines AI as 'the ability of machines to perform tasks that normally require human intelligence'.[7] Specific examples include 'recognising patterns, learning from experience,

5 Gray and Ertan, 2021, p. 6.

6 This problem is also emphasized when discussing lethal autonomous weapons system. For instance, Tadeo and Blanchard (2021) analysed existing definitions of autonomous weapons systems and concluded that different countries and organisations focus on different elements, leading to different approaches in addressing legal and ethical problems posed by these systems, p. 12.

7 U.S. Department of Defense, 2019, p. 5.

drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems'. Similarly, the United Kingdom (UK) 2022AI strategy sees AI as 'a family of general-purpose technologies, any of which may enable machines to perform tasks normally requiring human or biological intelligence, especially when the machines learn from data how to do those tasks'.[8] The 2019 French Ministry of Defence, AI strategy (see below) suggests AI processes are 'mechanisms of cognition and thought and use a combination of hardware and software to imitate them in order to assist or replace human activities'.[9]

The potential military and defence applications of these technologies seem almost unlimited, and many authors and organisations have attempted to provide some structure and classify the possible uses of AI for military and defence purposes according to certain criteria. At the most basic level, some policy documents differentiate between warfighting and other uses of AI in the military.[10] Rickli and Mantellassi consider that AI can serve as an analytical enabler (such as using AI for important data analysis), as a disruptor (using technologies such as deepfakes to produce and spread disinformation and otherwise disrupt institutions and processes), and as a force multiplier (using AI in weapon systems).[11] Gray and Ertan focus on technologies, categorising AI and autonomous systems into autonomous vehicles, autonomous air and missile systems, autonomous missiles, AI-enabled aircraft, data analytics, and logistics and personnel management.[12] Taddeo et al. differentiate between the uses of AI for sustainment and support,[13] non-kinetic adversarial uses (defensive and offensive cyber operations), and kinetic adversarial uses (decision-making leading to the use of force, LAWS, and supporting tactical decisions and personnel in combat).[14]

The aim of this chapter is to examine how the European legal framework might address the use of AI for military and defence purposes. Therefore, it is necessary to define the issues of using AI, which are important from a regulatory perspective. To do so, we briefly analyse the existing strategies covering AI in the military and defence sectors of NATO Member States.

The *NATO Artificial Intelligence Strategy* (NATO AI Strategy) was published in 2021.[15] There are plans to update this strategy to include issues such as generative AI.[16] The strategy calls for AI to be mainstreamed, ensuring that its development and use are undertaken responsibly, while at the same time safeguarding against threats

8 UK Ministry of Defence, 2022.
9 French Ministry of Defence, 2019, p. 3.
10 Devitt et al., 2020, p. 4.
11 Rickli and Mantellassi, 2023, p. 22.
12 Gray and Ertan, 2021, pp. 19–21.
13 Encompassing AI for system's robustness and resilience; to support back-office operations; to support logistics and operational planning; for situational awareness; for peacekeeping; for national contingency operations. Taddeo et al., 2023, p. 163.
14 Taddeo et al., 2023, p. 163.
15 NATO, 2021a.
16 Gosselin-Malo, 2023.

from the malicious use of AI by state and non-state actors.[17] The first goal is defined based on the Principle of Responsible Use, which includes lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation.[18] Second, it is recognised that adversaries and non-state actors might interfere with allied AI programmes using manipulation or sabotage; hence, it is necessary to protect against such events. It is further recognised that AI can also impact critical infrastructure and civil capabilities and preparedness, creating potential vulnerabilities.[19] Finally, the threat of disinformation campaigns using AI has also been recognised.[20]

The 2019 *Artificial Intelligence in Support of Defence* (French AI strategy) references compliance with the laws of war, armed conflicts, and other indirectly relevant rules.[21] Notably, France considers that contrary to certain popular misconceptions, AI has a potential which, properly managed and controlled, will help the French armed forces to take better account of the fundamental principles of the law of armed conflict because it can help mitigate discrimination between combatants and non-combatants, apply the principle of proportionality, and guarantee that action is determined strictly by need.[22] Finally, an important part of the French strategy is data governance. France recognises that the development and use of AI systems is dependent on access to vast, reliable, and up-to-date datasets. In this context, the French strategy recognises the difference between personal and non-personal data, and specifically mentions compliance with the General Data Protection Regulation (GDPR).[23]

The UK published its *Defence Artificial Intelligence Strategy* in 2022.[24] The UK generally considers that 'progress in AI must be achieved responsibly and safely according to democratic norms and the rule of law'.[25] It also emphasises the rule of international law, considering that it:

> provides a robust, principle-based framework for the regulation of weapons development and use, focusing on effects rather than the nature of any particular technology. It imposes positive obligations that take account of core principles – distinction, necessity, humanity and proportionality – and is the most appropriate way of regulating new means and methods of warfare.[26]

17 NATO, 2021a, para 3.
18 Ibid., para. 9.
19 Ibid., para. 16.
20 Ibid., para. 17.
21 French Ministry of Defence, 2019, pp. 5–6.
22 Ibid., p. 6.
23 Ibid., pp. 12–13.
24 UK Ministry of Defence, 2022.
25 Ibid., p. 11.
26 Ibid., p. 53.

Like France, the UK has expressed its commitment to work under the UN *Convention on Certain Conventional Weapons*.[27]

The European Union (EU) does not have a unified strategy for AI in its defence and military domains.[28] This is not surprising, considering the complex division of competences and interests between the EU and its Member States and various EU institutions. Consequently, it is hardly surprising that the EU's strategic thinking on the use of AI in the defence and military domains is not as coherent as NATO's and the national strategies mentioned above. However, this is not to say that it is impossible to discern some general positions of the EU in relation to the AI issues analysed in this report. However, as the overview below shows, it seems more appropriate to speak about the positions and policies of specific institutions in relation to specific AI issues than to say that there is a coherent and over-reaching strategy in this domain.

In 2018, the European Commission published a strategy, *Artificial Intelligence for Europe*, broadly outlining the state of development and policy aims in this area. This document called for many specific measures to boost the European EU's capacity for AI. An important aspect of this strategy is that the measures were designed to boost access to data, which is crucial for developing AI. From a legal perspective, AI is seen as being at least partially regulated by the existing rules at that time, primarily those covering personal data protection and the regulation of the flow of non-personal data. This calls for the development of appropriate ethical standards and criteria to ensure safety and liability. However, when it comes to the issue of AI in the defence and military domains, the 2018 strategy remains silent. The only mention of these issues is in relation to the work of international organisations, and it is mentioned that the use of AI in military domains is being discussed in these forums.[29]

In 2019, a team of AI experts established by the European Commission prepared a report on *Ethics Guidelines for Trustworthy AI*. In this report, the use of lethal autonomous weapon systems (LAWS) was highlighted as a critical concern. In this context, the Commission endorsed the position of the European Parliament and called for:

> the urgent development of a common, legally binding position addressing ethical and legal questions of human control, oversight, accountability and implementation

27 Ibid., p. 53.

28 Soare summarizes the current EU position as follows: 'Europeans lack a common AI integration strategy in defence which links technological power to strategic autonomy in terms of operational advantage against and competitiveness with other rival great powers. The EU does not have, nor does it currently plan to develop a common European military strategy to integrate AI in cyber and cross- domain military operations for operational and strategic advantage and it does not possess a common, regular threat and opportunity assessment based on European intelligence about its rivals' AI military innovation efforts and other international actors' geopolitical needs. The EU is not politically ready – or interested – to develop the kind of military capabilities, enablers, and legal powers to conduct algorithmic warfare'. Soare, 2023a, p. 78.

29 European Commission, 2018.

of international human rights law, international humanitarian law and military strategies.[30]

In 2020, the European Commission published a white paper, *On Artificial Intelligence – A European Approach to Excellence and Trust*.[31] This paper identified the key legal challenges to the deployment of AI, including compliance with fundamental rights and freedoms, risks to safety, and the functioning of the liability regime. Finally, it calls for establishment of a clear legal framework for the development and use of AI in the EU. However paper clearly states that 'it does not address the development and use of AI for military purposes'.[32]

The position of the European Parliament appears to differ. The parliament has addressed the issue of AI use in the defence and military sectors multiple times. Most of these interventions focus on the use of LAWS; however, some broader concerns and policy positions have also been articulated. In 2020, the parliament developed a framework to tackle the ethical aspects of AI, robotics, and related technologies.[33] This resolution elaborates on the positions of parliaments regarding the use of AI in the security and defence domains. In essence, the parliament maintained its earlier position regarding the use of LAWS without meaningful human control. Broader than that, it insists on respect for all applicable laws, including international humanitarian law, international human rights law, and EU law, in all situations where AI is used for defence purposes. However, the parliament also recognises the benefits of AI in the defence and military sectors, such as "higher quality collected data, greater situational awareness, increased speed for decision-making, reduced risk of collateral damage thanks to better cabling, protection of forces on the ground, as well as greater reliability of military equipment and hence reduced risk for humans and of human casualties".[34]

Interestingly, the use of AI in the defence and military sectors has attracted the attention of some EU Member States. For instance, during the Finnish presidency in 2019 Finland, Estonia, France, Germany, and the Netherlands published a food for thought paper on digitalization and artificial intelligence in defence.[35] In addition to seeking to open general discussions on disruption and transformation in defence and the impact of AI on military capabilities, this paper also addressed some regulatory issues. Generally, the paper seems to oppose a categorical ban on AI or autonomous systems and instead proposes that autonomous weapon systems be discussed and agreed upon internationally, specifically in the UN CCW forum.[36]

30 European Commission, 2019.
31 European Commission, 2020.
32 European Commission, 2020, p. 1.
33 European Parliament, 2020.
34 European Parliament, 2020, para. 93.
35 *Digitalization and Artificial Intelligence in Defence*, 2019.
36 Ibid., p. 2.

In 2022, the EU adopted *A Strategic Compass for Security and Defence*, which outlines the EU's future security and defence agenda.[37] It calls for the development of capabilities in the land, maritime, air, space, and cyber domains. AI is viewed as a part of the cyber domain, and it is proposed that the EU will 'develop and make intensive use of new technologies, notably quantum computing, AI and Big Data, to achieve comparative advantages, including in terms of cyber responsive operations and information superiority'.[38] Moreover, it calls for stepping up efforts at the national and EU levels to better prepare for the future battlefield and next-generation technology.[39]

Finally, the issue of regulating AI in military, defence, and national security contexts became the subject of discussion in the drafting process of the EU AI Act.

3. The legal and regulatory landscape for the use of AI in European military and defence sectors

Some key global issues and challenges posed by AI in the defence and military sectors have been outlined above (and in other chapters of this book). We now consider the regulatory and legal landscape within which those issues and challenges must be addressed in the EU. Initially we can note that the EU appears to be recognised for its strict regulatory requirements. For instance, the French AI strategy describes the EU as:

> an aspiring intermediate power … whose hardline approach to legal and ethical issues may be a strength or a weakness depending on its impact (standard-setting power underpinned by many public- and private-sector actors vs risk of having a research or entrepreneurial development policy that is too timid or hampered by excessive regulation).[40]

Soare is even more direct when she argues that 'European states exhibit self-imposed ethical and legal restraints, bordering on cultural-technological conservatism, which inhibits an ambitious European agenda on adopting military AI'.[41]

In this section, we discuss legal issues, which might impact the use of AI in the military and defence.

37 European Union External Action, 2022.
38 Ibid., p. 45.
39 Ibid., p. 48.
40 French Ministry of Defence, 2019, p. 7.
41 Soare, 2023b, p. 81.

3.1. Lethal autonomous weapons systems

One theme which features prominently in strategic documents and discussions on the use of AI in the military is the use of LAWS. There appears to be a consensus that these systems represent a particularly significant risk. However, there are different positions in terms of deployment and use. For instance, it is explicitly stated in the French strategy that France 'has no plans to develop fully autonomous systems where human operators have no control over the definition and performance of their missions', but at the same time it is against a preventive ban because it considers that such a ban "would hinder responses to legal and ethical challenges raised by them".[42] Other countries do not exclude the possibility of developing and using autonomous weapons systems with varying degrees of involvement.

Moreover, it appears that the most important part of the debate is the definition of LAWS. For instance, when Taddeo and Blanchard (2021) analysed the policies and documents of countries participating in discussions on LAWS in the UN Convention on Certain Weapons, they identified 12 definitions of LAWS.[43] Therefore, even if an international consensus on banning some fully autonomous systems emerges (which thus far seems unlikely), the issue of what constitutes such systems should first be resolved.

The EU law is understandably silent on the issue of LAWS. There is no EU law on the use of arms, and therefore no EU legal framework on the use of LAWS. However, some policy considerations have been expressed, most importantly by the European Parliament.

In 2014, the European Parliament passed a resolution on the use of armed drones, in which it, *inter alia*, called for a ban on the 'development, production, and use of fully autonomous weapons which enable strikes to be carried out without human intervention'.[44] This issue was addressed more comprehensively in 2018 in the resolution on autonomous weapon systems, in which the parliament called for 'a common position on LAWS that ensures meaningful human control over the critical functions of weapon systems, including during deployment, and to speak in relevant forums with one voice and act accordingly'.[45]

In 2019, the expert team on Artificial Intelligence established by the European Commission, stated in its *Ethics Guidelines for Trustworthy AI* that the development of LAWS 'could lead to an uncontrollable arms race on a historically unprecedented level and create military contexts in which human control is almost entirely relinquished, and the risks of malfunction are not addressed'.[46]

42 French Ministry of Defence, 2019, pp. 8, 10.
43 Taddeo and Blanchard, 2021, p. 7.
44 European Parliament, 2014.
45 European Parliament, 2018.
46 European Commission, 2019, p. 34.

Finally, in 2020, the European Parliament passed a resolution on the issue of a framework for the ethical aspects of AI, robotics, and related technologies.[47] This resolution elaborates on the position of the parliament regarding the use of AI in the security and defence domains. In essence, the parliament maintains its earlier position regarding the use of LAWS without meaningful human control and calls for international regulation of the development and use of fully autonomous, semi-autonomous, and remotely operated LAWS. The position of the parliament is that development, production and use of LAWS enabling strikes to be carried out without meaningful human control and that systems without respect for the human-in-the-loop principle' should be prohibited. The crucial elements in the position of parliament are human control and accountability.

Regarding human control, the parliament states that human control must be present in all phases of the design, development, deployment, and use of AI systems.[48] In particular, it is necessary that '…humans retain the agency to detect and disengage or deactivate deployed systems should they move beyond the mission framework defined and assigned by a human commander, or should they engage in any escalatory or unintended action'.[49] Generally, the position of the parliament is that 'human control should remain effective for the command and control of AI-enabled systems, following the human-in-the-loop, human-on-the-loop and human-in-command principles at the military leadership level'.[50]

This is further extended by the need for accountability. In this context the parliament 'stresses the need to establish clear and traceable authorisation and accountability frameworks for the deployment of smart weapons and other AI-enabled systems'.[51] More specifically, it 'considers that AI-enabled systems, products and technology intended for military use should be equipped with a "black box" to record every data transaction carried out by the machine'.[52]

However, while the policy considerations of the European Parliament seem to be well developed and reasonable, the fact remains that they are not binding in any formal way. As explicitly confirmed in the EU's AI Act, the use of AI in the military context is determined by the specificities of the Member States' and the EU defence policies, which are subject to public international law.[53] Therefore, it recognises that international law is the appropriate legal framework for the regulation of AI systems in the context of the use of lethal force.[54]

47 European Parliament, 2020.
48 European Parliament, 2020, para. 102.
49 European Parliament, 2020, para. 101.
50 European Parliament, 2020, para. 102.
51 Ibid.
52 European Parliament, 2020, para. 101.
53 AI Act, Recital 24.
54 AI Act, Recital 24.

3.2. General regulation of AI

The EU is sometimes considered a global regulatory champion, and not without reason. Very high regulatory standards have been set in sectors such as personal data protection and the use of data in general, online content, and online platforms. The same applies to regulation of AI.

Following its 2020 White Paper on AI and many other policy papers and proposals issued by multiple EU institutions over the past several years, the European Commission prepared a draft for a comprehensive regulatory framework for AI. Hence, a proposal for a regulation laying down harmonised rules on AI, better known as the Artificial Intelligence Act, was published in April 2021 (2021 AI Act draft).[55] This document has been extensively debated and amended. For the purposes of the analysis in this chapter, it is important to consider the proposal which was prepared during the Slovenian presidency, in November 2021 (2021 AI Act compromise).[56] The latest publicly available official version was adopted by the European Parliament on 13 March 2024 (hereinafter, the AI Act).[57] While this version is yet to undergo a final legal and linguistic analysis and a formal endorsement by the Council of the EU, it can be expected that it will not undergo further significant changes. Therefore, we refer to the March 2024 version of the AI Act in this chapter.

The key question is, what might be the impact of the AI Act on the development and use of AI systems in the military and defence sectors? To address this question, it is necessary to consider the scope of the AI Act, which excludes most AI systems used in the military and defence, and the possible impact of the Act on the development of dual-use AI systems.

3.2.1. Situations where the AI Act does not apply

Based on the first draft of the AI Act in 2021 excluded certain systems used for military purposes from its scope. However, two subsequent publicly available texts show that the thinking behind this provision evolved and that the provision itself became both broader and more precise.

The 2021 draft provided in Article 2(3) that '[t]his Regulation shall not apply to AI systems developed or used exclusively for military purposes', which seems relatively clear but is, in effect, very limited. First, it should be noted that the 2021

55 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence *(Artificial Intelligence Act)*, 2021. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf (Accessed: 5 February 2024).

56 Ibid.

57 *European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, 2021. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7536_2024_INIT (Accessed: 5 February 2024).

draft did not contain a provision regarding which legislative acts of the EU do not apply to an activity which falls outside the scope of EU law, which is otherwise ordinarily used in EU legislation. Secondly, it was declared that the AI Act would not apply to 'systems developed or used exclusively for military purposes', but there was no mention of defence purposes. Since one might argue that there are substantial differences between military and defence purposes, with the latter being broader, this exception could have indeed been limited. Finally, the scope of Article 2(3) was further elaborated on in Recital 12, where it was explained as follows:

> AI systems exclusively developed or used for military purposes should be excluded from the scope of this Regulation where that use falls under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU).

It would, therefore, follow that if Article 2(3) was interpreted in line with Recital 12, AI systems developed for military purposes would be excluded from the scope of the AI Act only under the condition that they were used for activities falling under the remit of the Common Foreign and Security Policy as regulated by the Treaty on the European Union (TEU). This would once again significantly limit the scope of exceptions because it would not cover national military activities which are not part of the CFSP.

In November 2021, during the Slovenian presidency, a compromise text was drafted that included substantial amendments to the scope of the AI Act. Most importantly, Article 2(3) was broadened to include national security, so that it read '[t]his Regulation shall not apply to AI systems developed or used exclusively for military or national security purposes'. Moreover, the relevant Recital was also amended to explain the following:

AI systems exclusively developed or used for military purposes should be excluded from the scope of this Regulation. Such exclusion is justified by the specifities of the Member States' and the common Union defence policy subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military activities. Nonetheless, if an AI system developed exclusively for military purposes is used outside those purposes, such system would fall within the scope of this Regulation. … When AI systems are exclusively developed or used for national security purposes, they should also be excluded from the scope of the Regulation, taking into account the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU.

Finally, in the version of the AI Act adopted in March 2024, Article 2(3) regarding exclusions from the scope was also amended, and now reads as follows:

> This Regulation does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national

security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.
This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.
This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

Moreover, Recital (24) was also changed and now reads as follows:

If and insofar AI systems are placed on the market, put into service, or used with or without modification of such systems for military, defence or national security purposes, those should be excluded from the scope of this Regulation regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity. As regards military and defence purposes, such exclusion is justified both by Article 4(2) TEU and by the specificities of the Member States' and the common Union defence policy covered by Chapter 2 of Title V TEU that are subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. As regards national security purposes, the exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities. Nonetheless, if an AI system developed, placed on the market, put into service or used for military, defence or national security purposes is used outside those temporarily or permanently for other purposes, for example, civilian or humanitarian purposes, law enforcement or public security purposes, such a system would fall within the scope of this Regulation. In that case, the entity using the system for other than military, defence or national security purposes should ensure compliance of the system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for an excluded purpose, namely military, defence or national security, and one or more non-excluded purposes, such as civilian purposes or law enforcement, fall within the scope of this Regulation and providers of those systems should ensure compliance with this Regulation. In those cases, the fact that an AI system may fall within the scope of this Regulation should not affect the possibility of entities carrying out national security, defence and military activities, regardless of the type of entity carrying out those activities, to use AI systems for national security, military and defence purposes, the use of which is excluded from the scope of this Regulation. An AI system placed on the market for civilian or law enforcement

> purposes which is used with or without modification for military, defence or national security purposes should not fall within the scope of this Regulation, regardless of the type of entity carrying out those activities.

Compared to the 2021 version, the 2024 Draft AI Act defines exemptions from the scope more broadly and precisely. Several important points should be noted. First, Article 2(3) now explicitly excludes AI-related activities in areas outside the scope of EU law from the scope of the Act. This is in line with other EU legal instruments in the fields of electronic communications, personal data, non-personal data analysed in this chapter. To further clarify, it is explicitly stipulated that AI systems which are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes are excluded from the scope of the AI Act. The same goes for AI systems which are not placed on the market or put into service in the EU, provided that the output is used exclusively for military, defence or national security purposes in the EU.

Second, the AI Act makes it explicit in Article 2(3) that exclusions from its scope apply regardless of the type of entity entrusted by the Member States to carry out the tasks in relation to those competences. This seems especially important for at least two reasons. First, developers of AI systems are usually private entities, so it is useful to clarify that when those entities are acting in national security, defence or military domains for the benefit of Member States, the exceptions still apply. Second, this solution also addresses the issues the CJEU had in some personal data protection cases (see a more extensive discussion below), when it concluded *inter alia* that the exception of national security does not apply when data processing is conducted by private entities (service providers) and not by the Member States themselves (or more precisely, by state bodies).

Considering the legislative history, explanations provided in the Recitals, and generally the efforts which went into drafting what is now Article 2(3), it seems clear that the drafters intended to ensure broad exemption for the use of AI systems in the national security, defence and military sectors. The main consequence of this approach is that the use of AI in those domains remains within the competence of Member States presumably outside the control of the CJEU. The first point seems uncontroversial since it is obvious that in those areas where the EU does not have competence and which are excluded from the scope of secondary EU laws, Member States can legislate freely. Therefore, starting from the premise that any limitations in the development and use of AI capabilities for defence and military sectors can be seen as a self-imposed restraint, it seems that EU law addresses this properly and essentially empowers Member States to decide for themselves.

However, the second and much more complicated question is: are the actions of Member States still under the control of the CJEU? Based on the approach previously pursued by the CJEU, it appears that the answer might be affirmative, at least in part. The CJEU has been explicit many times in cases regarding national security. For example:

> Although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.[58]

Similarly, and specifically in the context of the armed forces, the CJEU concluded in *Sirdar v. The Army Board and Secretary of State for Defence* that:

> "decisions taken by Member States in regard to access to employment, vocational training and working conditions in the armed forces for the purpose of ensuring combat effectiveness do not fall altogether outside the scope of Community law".[59]

Moreover, in *Kreil v. Bundesrepublik Deutschland,* the CJEU used the same approach as in *Sirdar* ***v.*** *The Army Board and Secretary of State for Defence* concluded that while it is for Member States to make decisions on the organisation of their armed forces, this does not mean that such decisions fall entirely outside the scope of EU law *per se*.[60] Consequently, CJEU considered that it is competent to verify 'whether the measures taken by the national authorities in the exercise of their recognised discretion did, in fact, have the purpose of guaranteeing public security and whether they were appropriate and necessary to achieve that aim'.[61] Following its analysis, the CJEU concluded that EU law precluded national measures providing for the general exclusion of women from military posts involving the use of arms.

The same principles were also confirmed in the *Dory v. Bundesrepublik Deutschland*[62] case, where the CJEU repeated that it is competent to supervise the decisions of national authorities in the area of guaranteeing public security, but at the same time, confirmed that community law does not preclude compulsory military service being reserved for men. It appears that one of the reasons for such a conclusion (and different from the *Kreil v. Bundesrepublik Deutschland* case) was that there are no provisions governing 'the Member States' choices of military organisation for the defence of their territory or of their essential interests' in EU law, while (as in *Kreil v. Bundesrepublik Deutschland*) 'the principle of equal treatment of men and women in connection with employment, including access to military posts', is subject to EU law.

Finally, in the recent case of *B. K. v. Republika Slovenija* (2021), the CJEU was asked to answer several questions regarding the application of Directive 2003/88/EC concerning certain aspects of the working hours for an officer in the Slovenian army.

58 C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others v. Premier minister and Others*), para. 99, and cases cited there.
59 C-273/97 (*Sirdar v. The Army Board and Secretary of State for Defence*), para. 21.
60 C-285/98 (*Kreil v. Bundesrepublik Deutschland*), para. 15.
61 C-186/01 (*Dory v. Bundesrepublik Deutschland*), para. 34.
62 Ibid.

Once again, it was argued that EU law does not apply to the military on the basis of Article 4(2) of the TEU, and once again, the CJEU concluded otherwise, stating that the provision in question does not exclude the working hours of military personnel from the scope of EU law.[63] According to the court, Article 4(2) of the TEU requires:

> application to military personnel of the rules of EU law relating to the organisation of working time is not such as to hinder the proper performance of those essential functions. Therefore, those rules cannot be interpreted in such a way as to prevent the armed forces from fulfilling their tasks and, consequently, so as adversely to affect the essential functions of the State, namely the preservation of its territorial integrity and the safeguarding of national security.

Thus, the CJEU set specific criteria for determining when the directive governing working hours for military personnel would be applied or excluded.

While the cases mentioned above are not directly related to the use of AI in the military or defence arenas, applying the same logic about competencies suggests that the CJEU might not accept that any use of AI in national security, defence or military sectors is excluded from its scope of its review. Hence, the real question is probably how active the court will be in setting the boundaries of the permissible use of AI in these sectors.

For instance, it seems reasonable to think that the use of LAWS should not be subject to any scrutiny by the court. However, what about other AI systems that might be used in the military or defence, such as personnel management, logistics, training optimisation, situational awareness, and threat analysis? Recital 24 specifically mentions AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. Therefore, it appears that the legislative intent here was to create broad exceptions to the application of AI in the national security, defence, and military domains.

While fully accepting the principle that exceptions must be interpreted narrowly, it seems correct to also consider positions of the institutions involved in drafting the AI Act, which obviously intended for Member States to retain significant, if not full, discretion over the use of AI in defence and military sectors. The drafting process highlighted the difficulty of legislating in a rapidly changing technological environment like AI. A parallel can be drawn with the CJEU's handling of causes related to the surveillance of electronic communications metadata, where the Court initially set conditions for lawful retention but then had to clarify and refine its approach over numerous cases. For these reasons, it would be preferable to see the CJEU exercising its powers very cautiously when addressing the inevitable questions about the use of AI in military and defence domains.

63 C-742/19 (*B.K. v. Republika Slovenija*), para. 46.

3.2.2. Situations where the AI Act applies

The AI Act is ambitious and seeks to promote elements of market regulation of AI while at the same time promoting 'human-centric and trustworthy artificial intelligence'[64] and protecting health, safety, fundamental rights, democracy, and the rule of law. Most importantly, the Act seeks to protect against the harmful effects of AI systems.[65] To what extent will all of this be achievable is yet to be seen, but there is no denying that the legislative aims are set high. In this chapter, we only briefly outline the main elements and approaches of the AI Act. The Act regulates the use of AI systems and subjects them to strict regulatory requirements.

3.2.2.1. AI systems

The definition of an AI system has changed significantly through legislative procedures. In the final version adopted by the Act, an AI system is defined as follows:

> A machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[66]

From the above definition, we see that the main characteristics of an AI system are that it is (1) machine-based, (2) has ability to infer, (3) autonomy, and possibly, but not necessarily, exhibits adaptiveness.

First, the AI system is machine-based, which pursuant to Recital 12, simply denotes the fact that AI systems run on machines. It will obviously include software, which was the term used in the 2021 AI Draft Act, provided that the requirements regarding autonomy and the ability to infer are satisfied. It appears that one of the reasons for removing the word "software" was to make it explicit that AI systems do not include 'simpler traditional software systems or programming approaches' or 'systems that are based on the rules defined solely by natural persons to automatically execute operations'.[67]

Secondly, and connected to the above, a key defining element of an AI system is its ability to infer, which is defined as 'the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments', as well as the 'capability of AI systems to derive models

64 AI Act, Recital 1.
65 AI Act, Article 1(1).
66 AI Act, Article 3(1).
67 AI Act, Recital 12.

or algorithms from inputs or data'.[68] Moreover, it is explained that the capacity of an AI system to infer:

> transcends basic data processing' and 'enables learning, reasoning or modelling'.[69] This can be achieved by techniques which 'include 'machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved.[70]

Third, AI systems operate with varying levels of autonomy. They have 'some degree of independence of actions from human involvement and of capabilities to operate without human intervention'.[71] Finally, AI systems may (but do not have to) exhibit adaptiveness, which refers to 'self-learning capabilities, allowing the system to change while in use'.[72]

The AI Act regulates three categories of AI systems: (1) those which encompass prohibited AI practices, (2) high-risk AI systems, and (3) other AI systems.

3.2.2.2. Prohibited AI systems

Prohibited AI systems are those which support manipulative, exploitative and social control practices.[73] They include (under certain conditions) AI systems which:

- Are manipulative, in the sense that they (a) seek to influence behaviour of a person or a group of persons, inducing them to take decisions they would not otherwise taken, and thereby causing them significant harm, or creating a likelihood of such harm, or (b) exploit any of the vulnerabilities due to age, disability of specific social or economic situation, leading to a distortion of behaviour causing them significant harm, or creating a likelihood of such harm.[74]
- Provide for social scoring of natural persons.[75]
- Are used for assessing or predicting the likelihood of a natural person committing a criminal offence.[76]
- Create of expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.[77]

68 AI Act, Recital 12.
69 Ibid.
70 Ibid.
71 Ibid.
72 Ibid.
73 Ibid., Recital 28.
74 Ibid., Article 5(1)(a,b).
75 Ibid., Article 5(1)(c).
76 Ibid., Article 5(1)(d).
77 Ibid., Article 5(1)(e).

- Infer emotions of natural persons in workplace and in education institutions.[78]
- Enable biometric categorisation of persons on the basis of specific criteria.[79]
- Provide for real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes.[80]

The systems mentioned above are considered particularly harmful, abusive, and contrary to the EU's fundamental values, democracy, and individual human rights and freedoms. Consequently, it is prohibited to place them on the market, put them into service, or use them. Placing on the market is defined as making available on the market for distribution or use 'in the course of a commercial activity, whether in return for payment or free of charge'. Therefore, it appears that the prohibition becomes operative only when an AI system has already been developed and becomes available for use. For instance, the AI Act does not seem to preclude the development of a system which can infer the emotions of military personnel in certain high-stress situations. Further, because placing AI systems exclusively for military, defence, and national security purposes in the market is excluded from the scope of the AI Act, we can see that the development and use of generally prohibited AI systems might be possible in these domains. This is an example of a situation where legal challenges could occur. For instance, courts might think about the usage of AI emotion recognition systems for selecting military personnel for certain functions and whether that would be considered a matter falling fully within Article 4(2) of the TEU, or a matter where the court could exercise its competence and possibly provide some guidance.

3.2.2.3. High-risk AI systems

Following prohibited AI practices, the next category is high-risk AI systems. These are products, or safety components of products,[81] specifically listed in the AI Act and regulated under EU law.[82] They include such items as machinery, toys, lifts, some medical devices, products in the field of aviation security, and some vehicles. High-risk AI can also be specific systems[83] in biometrics; critical infrastructure; education and vocational training; employment; workers management; access to and enjoyment of essential private services and essential public services and benefits; law enforcement; migration, asylum and border control management; administration of justice and democratic processes.[84]

78 Ibid., Article 5(1)(f).
79 Ibid., Article 5(1)(g).
80 AI Act, Article 5(1)(h).
81 Ibid., Article 6(1).
82 Ibid., Annex II.
83 Ibid., Article 6(2a).
84 Ibid., Annex III.

High-risk AI systems are subject to strict regulatory requirements, which form a significant part of the regulations. These include having appropriate risk management systems, rules on using data for training AI models, documentation and record-keeping, transparency and providing information to deployers, accuracy, robustness and cybersecurity. These obligations generally seek to ensure that high-risk AI systems are trustworthy.

3.2.2.4. Other AI systems

The AI Act also contains obligations for AI systems which are neither specifically prohibited nor high-risk but still require additional regulations. First, where an AI system (for instance, a chatbot or virtual assistant) is intended to interact directly with natural persons, there is, with some exceptions, a duty to inform the person that they are interacting with an AI system.[85]

Secondly, providers of AI systems which generate synthetic audio, image, video or text content, have an obligation to ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated.[86] Similarly, deployers of AI systems that generate or manipulate image, audio, or video content constituting "deep fake", or those which generate or manipulate text published for the purpose of informing the public, must disclose that the content has been artificially generated or manipulated.[87]

Third, deployers of an emotion recognition system or biometric categorisation system must inform natural persons exposed to the operation of the system and process their data in accordance with personal data protection rules.[88]

3.2.2.5. General-purpose AI models

General purpose AI models are regulated by a separate set of provisions under the AI Act. Pursuant to a definition in Article 3(66) of the AI Act, the general-purpose AI model is:

> an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are released on the market.

85 Ibid., Article 50(1).
86 Ibid., Article 50(2).
87 Ibid., Article 50(4).
88 Ibid., Article 50(3).

The key characteristics of general-purpose AI models are that they are capable of significant generality and able to competently perform a wide range of distinct tasks.[89] Furthermore, they can, but do not have to be, trained with large amounts of data using different methods. And while generality and the ability to perform a wide range of tasks can be determined by various factors, 'models with at least a billion of parameters and trained with a large amount of data using self-supervision at scale' are considered to satisfy those conditions.[90] Typical examples of general-purpose AI models are those which allow for 'flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks'.[91]

As explained in Recital 97, although AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems. Hence, if an AI model which allows image processing is integrated as a safety component in an autonomous car, it becomes part of an AI system. Providers of general-purpose AI models are subject to multiple obligations, including ensuring transparency of their models. Hence, with some exceptions, they are required to publish up-to-date documentation about their models, address copyright issues, and explain how their models are trained.[92]

3.2.2.6. General-purpose AI models with systematic risks

Some general-purpose AI models are considered to pose systematic risks and are, therefore, subject to stricter regulatory regimes. General-purpose AI models pose a systematic risk if they possess certain technical capabilities or are capable of producing certain effects.[93] The specific determining criteria are provided in Annex XIII of the AI Act. In addition to obligations applicable to providers of all general-purpose AI models, providers of models with systemic risk must undertake additional duties regarding evaluation, risk assessment and mitigation, incident management, and cybersecurity.[94]

3.2.2.7. Impact on defence and military sectors

As previously discussed, the development and use of AI systems and general-purpose AI models are subject to strict regulatory requirements. Generally, there are no rules which would exclude the possibility of using an AI system or model in

89 See also Recital 97 of the AI Act.
90 AI Act, Recital 98.
91 AI Act, Recital 99.
92 AI Act, Article 53.
93 AI Act, Article 51.
94 AI Act, Article 55.

defence and military domains. In contrast, as elaborated above, Article 2(3) of the AI Act generally seeks to exclude the use of AI in these sectors from the scope of regulation. The main issue here might be that many AI systems have dual uses. For instance, an AI system used as a component in a civilian vehicle can at the same time be used for military vehicles. An AI model used to produce synthetic videos in the form of deep fakes can be used for civilian purposes or to lead a campaign aimed at achieving certain military aims. However, the AI Act generally contains sufficient rules to address these issues when it creates broad exclusions for the national security, military, and defence sectors.

It must be acknowledged that the AI Act will impose significant requirements on the AI industry, when it comes into force. And of course, if we compare Europe to jurisdictions with fewer or no regulations, then the legal framework for development and use of AI in Europe may appear more restrictive. However, whether these rules will seriously limit innovation and creativity and the use of AI products remains to be seen. Furthermore, AI technology is itself just one part of the equation. Another one is the data processed by AI which might be an area with potentially an even bigger need for legal regulation.

3.3. AI as an analytical enabler: processing of data

One of the most promising uses of AI in the military is in the intelligence, surveillance, and reconnaissance domains. In this context, AI acts as an analytical enabler, making it possible to analyse substantial quantities of data, including live data, which would otherwise require disproportionate amounts of work by human analysts.[95] Similarly, Nurkin stated that:

> near ubiquitous and networked sensors embedded in equipment and in human operators will collect massive amounts of data that could overwhelm the capacity of humans to process – be it video, images, biometric data, signals intelligence, geospatial intelligence, or other types of information.[96]

According to the French AI strategy, AI is used in applications which aim to detect and recognise data, predict future outcomes, seek correlations in order to deduce a generic form of behaviour or flag up abnormal behaviour, and optimise solutions to problems such as logistical flows or flight paths.[97]

All these factors are highly dependent on the availability of reliable data. This is explicitly recognised by NATO, which is addressing this issue through its Data Exploitation Framework Policy. The purpose of this policy is to 'ensure that NATO is able to leverage data as a strategic resource' and to improve the data exploitation

95 Rickli and Mantellassi, 2023, p. 19.
96 Nurkin, 2023, p. 37.
97 French Ministry of Defence, 2019, p. 3.

capabilities across all levels in the military, civilian, and political domains'.[98] By doing so, the alliance aims to achieve multiple goals, including information superiority and data-driven decision-making at all levels.[99] This Policy makes explicit reference to NATO's AI Strategy; therefore, it is obvious that one of the purposes of the data exploitation policy is to support the alliance's AI efforts.

The use of AI for data analytics purposes also features prominently in national strategic documents, and it is clear that data analytics can support both combat and noncombat operations. Regarding combat operations, AI is primarily expected to improve situational awareness and decision-making.[100] As explained in the U.S. 2018 strategy, 'AI can generate and help commanders explore new options so that they can select courses of action that best achieve mission outcomes'.[101] It is also recognised that the use of AI for analytics can contribute to compliance with the law of armed conflicts, because advanced analytics can improve the accuracy of military assessments and enhance mission precision, thereby reducing the risk of civilian casualties and other collateral damage.[102]

With regard to noncombat operations, the benefits of AI are manifold, including reducing inefficiencies in manual, laborious, and data-centric tasks, simplifying workflows, and improving the speed and accuracy of repetitive tasks.[103] It can increase the safety and supply of operating equipment, and streamline business processes.[104]

However, data can be a scarce resource for at least two reasons. First, some states might not have access to the same quantities of data because they do not have strong local data-centric industries. In this context, the French AI strategy states that:

> major digital players, especially American and Chinese, … have access to what really fuels AI: the vast mass of data that their customers provide to them free of charge at each interaction. Having initially sought to know their customers better in order to enhance their products and services, these actors are now using their very deep pockets to pursue greater ambitions, such as driverless cars, smart cities and personalised healthcare. Their products set the standard, and the sheer extent of their use cases makes them attractive to the military, especially in the many dual-use applications. As in the digital sphere as a whole, the defence sector does not necessarily blaze a trail but takes advantage of advances in civilian uses, adapting them to its own particular needs where necessary.[105]

98 NATO, 2021b, para. 1.1.
99 Ibid., para 2.1.
100 U.S. Department of Defense, 2019, p. 11.
101 Ibid., p. 11.
102 U.S. Department of Defense, 2019, p. 6.
103 Ibid., p. 6.
104 Ibid., p. 11.
105 French Ministry of Defence, 2019, p. 4.

Second, states operate under different legal requirements where the use of data is concerned. In some countries, there are no strong privacy or personal data protection laws, which consequently creates a more permissive environment for data processing. Others may be operating in different circumstances. As also noted in the French AI strategy, 'the collection and exploitation of data on a massive scale cannot be envisaged without strict compliance with prevailing personal data legislation, especially the GDPR'.[106] Likewise, the NATO Data Exploitation Framework Policy calls for 'data exploitation efforts aligned with core Alliance values, including the protection of personally identifiable information and privacy'.[107]

Globally, it is difficult to find a legal system which imposes stricter requirements for data processing than that of the EU. From the perspective of EU law, any piece of data is either personal or non-personal. Both categories are subject to legal regulations, with that governing the use of personal data being much more stringent. Moreover, specific rules are applicable to electronic communications data. Therefore, in the following sections, we consider whether and how the EU rules regulating the use of data can indirectly impact the use of AI systems.

3.3.1. Electronic communications data

Electronic communications are a rich source of data that can be used for law enforcement, national security, and defence purposes. For instance, surveillance of electronic communications is a method routinely used by investigative agencies all around the world when dealing with serious crime, and the same methods are also frequently used for national security purposes. Electronic communications data can be especially useful in the context of military operations. For instance, it was recently reported that the use of cell phones by a group of Russian soldiers enabled Ukrainian military to determine their location, leading to a deadly strike on the premises where they were located.[108] This is an obvious example of a military action taken on the basis of analysed electronic communications data, but such data can also be used outside of military conflicts, for various intelligence gathering, counter-intelligence and surveillance purposes in the context of national defence. And while in times of war accessing electronic data for defence purposes may not trigger legal concerns, the situation is different in peacetime when access to data still might be necessary.

When dealing with communications surveillance, it is useful to differentiate between content data and metadata. Content data is 'the meaning or purport of the communication, or the message or information being conveyed by the communication'.[109] Metadata can include various categories of technical data generated in the

106 Ibid., 2019, p. 13.
107 NATO, 2021b, para. 3.1.
108 *Unauthorized use of cellphones by Russian soldiers led to Ukrainian strike that killed 89 troops, military says*, 2023.
109 Council of Europe, 2001, para. 209.

course of the conveyance of communications. It includes what is sometimes designated as "traffic data" and "location data". For instance, in the Council of Europe's Convention on Cybercrime traffic data is defined as any data 'indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service'.[110] EU Directive 2002/58 defines it more generally as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.[111] The now invalidated EU Data Retention Directive had a detailed list of categories of data falling within this definition, including data indicating the source and destination of communication; the date, time duration, and type of communication, and the location and type of mobile communication equipment used.[112]

Tapping these data provides a rich source of information for state authorities in the domains of law enforcement, national security, and national defence. The interception of content data and the real-time monitoring of traffic data for criminal investigations and proceedings is explicitly envisaged at the European level by the Council of Europe's Convention on Cybercrime.[113] Almost all countries use similar powers based on domestic legislation for national security purposes.

In the EU, the Directive on Privacy and Electronic Communications (ePrivacy Directive) regulates the processing of personal data and the protection of privacy in the electronic communications sector. It applies to all publicly available electronic communications services in public communications networks in the EU,[114] but pursuant to Article 1(3), it does not apply to:

> activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Member States are required to ensure the confidentiality of communications and the related traffic data, and in particular prohibit 'listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data'.[115] Generally, traffic data must be erased or anonymised when they are no longer needed for communication transmission.[116] Location data can generally be processed anonymously or with the user's consent.[117] An exception, is prescribed in

110 *Convention on Cybercrime*, 2001, Article 1(d).
111 Directive 2002/58/EC, Article 2(b).
112 Directive 2006/24/EC, Article 5.
113 *Convention on Cybercrime*, 2001, Article 20.
114 Directive 2002/58/EC, Article 3.
115 Directive 2002/58/EC, Article 5(1).
116 Directive 2002/58/EC, Article 6(1).
117 Directive 2002/58/EC, Article 9(1).

Article 15(1) of this directive that Member States of the EU may legislate to restrict the scope of the above rules when such a restriction:

> constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.[118]

It is further explained that 'to this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph'.[119]

Articles 1(3) and 15(1) of the ePrivacy Directive appear to clearly exempt activities concerning core state functions, such as national security, national defence, and activities of the state in areas of criminal law, namely the prosecution of criminal offences, from safeguards defined in the directive. However, the situation is much more complicated. Member States are, among other exceptions to privacy and personal data protection in the context of electronic communications, permitted (per Article 15(1) of the ePrivacy Directive) to enact legislation requiring service providers to retain (proactively store) traffic data, for a limited period, on grounds which includes *inter alia* national security and defence. Several years after the ePrivacy Directive was enacted, the permission for Member States to provide for retention of data became their obligation, when the Data Retention Directive came into force in 2006. That directive now required Member States to adopt measures to ensure that traffic data (as defined in its Article 5) be retained for a period of not less than six months and not more than two years from the date of the communication.[120] The Data Retention Directive had a transposition period until 15 September 2007 which could have been extended by individual Member States to 2009 for internet access, internet telephony, and internet e-mail.

Although the Data Retention Directive envisaged the use of retained data primarily for law enforcement purposes, it did not limit access to retained data solely to state authorities acting in the criminal law domain. Instead, it was prescribed that the retained data be accessible to competent national authorities in specific cases and in accordance with national law.[121] Therefore, many Member States provided that in addition to law enforcement, authorities in the national security and defence sectors could also access and use the retained data.

For the next approximately seven years, the Member States were obligated to ensure that communication service providers retained traffic data for all their users and made it accessible to competent national authorities, as defined in national law.

118 Directive 2002/58/EC, Article 15(1).
119 Directive 2002/58/EC, Article 15(1).
120 Directive 2006/24/EC, Articles 3, 5 and 6.
121 Directive 2006/24/EC, Article 4.

Then in 2014, the Court of Justice of the EU (CJEU) invalidated the Data Retention Directive in *Digital Rights Ireland* case, on the account that it disproportionately interferes with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The court applied a strict necessity test and found the directive lacking, for multiple reasons.

After the Data Retention Directive was invalidated, the situation effectively reverted to that established by the ePrivacy Directive: Member States were permitted, but no longer obliged, to require service providers to retain data. However, this was only the beginning of the EU data retention saga. Two years after *Digital Rights Ireland*, the CJEU ruled in *Tele2 and Watson*[122] that national legislation which provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication is contrary to Article 15(1) of the ePrivacy Directive, interpreted in light of CFEU.[123]

Although the issue of the scope of restrictions mentioned in Articles 1(3) and 15(1) was occasionally raised before, in *La Quadrature du Net and Others v. Premier minister and Others* the CJEU was explicitly asked to rule, *inter alia*, whether general and indiscriminate retention of traffic and location data for, among other purposes of national security, territorial integrity, and national defence, is in violation of relevant EU law.[124] In these joined cases, several Member States advanced the argument that national legislation pursuing those aims falls outside the scope of the ePrivacy Directive on the basis of Article 1(3),[125] also considering the division of competences between the Union and its Member States, as defined in Article 4(2) of the Treaty on European Union (TEU). It was argued that activities of intelligence services 'in so far as they relate to the maintenance of public order and to the safeguarding of internal security and territorial integrity, are part of the essential functions of the Member States and, consequently, are within their exclusive competence'.[126]

However, the CJEU was not persuaded. In fairness, many of the problems stem from the fact that the ePrivacy Directive stipulates in Article 1(3) that activities concerning public security, defence, state security, etc., are exempt from its scope of application, and then in Article 15(1) allows Member States to, under certain conditions, restrict the scope of rights and obligations provided for in the directive for essentially the same purposes. Therefore, it seems logical to conclude that if all activities related to the security purposes of the state were exempted from the scope of the directive based on Article 1(3), there would be no need to regulate restrictions for those same purposes in Article 15(1). Therefore, the CJEU concluded that:

122 C-203/15 and C-698/15 (*Tele 2 and Watson*).
123 C-203/15 and C-698/15 (*Tele 2 and Watson*), para. 134.
124 C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others v. Premier minister and Others*), para. 84.
125 Ibid., para. 86.
126 Ibid., para. 89.

> Article 15(1) of Directive 2002/58 necessarily presupposes that the national legislative measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.[127]

However, the opposite is also true: if all activities in the security domain must satisfy the conditions under Article 15(1) of the Directive, then what would be the purpose of exempting those activities based on Article 1(3)?

The CJEU solves this conundrum by differentiating between data processing operations carried out by providers of electronic communications services, including operations resulting from obligations imposed on those providers by public authorities and operations directly implemented by Member States, without imposing processing obligations on service providers.[128] The first category is within the scope of the ePrivacy Directive and can be lawful under EU law, provided that conditions under Article 15 are satisfied. The second category is exempt from the ePrivacy Directive pursuant to Article 1(3).

What is important in this context is that the CJEU is explicit in explaining that the considerations of Article 4(2) of the TEU do not change the outcome. This is because the court maintains the position that:

> although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.[129]

It might be claimed that the issues surrounding the use of electronic communications metadata are only marginally relevant to the discussion of the use of AI in the military and defence sectors. However, that is so only on first sight. The core argument here is that the application of personal data protection rules, including those in electronic communications, has the potential to significantly impact data processing in those domains. In short, outcomes of the discussions on data retention in the EU are that Member States are precluded from ordering service providers to store electronic communication's metadata generally and indiscriminately, even when they are acting for national security purposes, which is fully in the domain of competences of the Member States. Furthermore, the CJEU set the standards for permissible data retention itself, by explaining in *Tele2 and Watson* that while general and indiscriminate data retention is prohibited, "targeted retention" (which

127 Ibid., para. 95.
128 Ibid., paras. 101, 103.
129 C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others v. Premier minister and Others*), para. 99.

is nowhere defined in EU law) might be permitted under certain conditions. It would take too much space in this chapter to define targeted retention, and discuss the legal problems caused by the approach mandated by the CJEU. In our view, the main message here is that the courts should not assume the role of legislators and should exercise their discretion moderately.

3.3.2. Personal data

The analysis above was limited to discussing the use of data from electronic communications, for the purposes of national security and defence. While this includes vast amounts of data which could be useful in the miliary and defence sectors, there are many more data being generated and processed outside of electronic communications. In legal terms, those other data might be considered "personal data" under applicable EU law. This category of data is currently regulated by the GDPR, which replaced the previously applicable Directive 95/46 in 2018.[130] If data is considered personal and is otherwise within the scope of the GDPR, then very strict regulatory regimes will apply to it.

Pursuant to Article 4(a) of the GDPR, personal data is defined as:

> any information relating to an identified or identifiable natural person („data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This might seem to be a straightforward concept, but once again the devil seems to be in the details. Personal data encompasses (1) any information which is (2) related to (3) an identified or identifiable (4) natural person.[131]

The notion of "any information" is very broad. Importantly, the rights to personal data protection and privacy are not synonymous.[132] Therefore, as was made explicit by the CJEU in *Client Earth,* 'the concepts of "personal data"… and of "data relating to private life" are not to be confused. Consequently, the claim … that the information at issue does not fall within the scope of the private life … is ineffective'.[133] Even if information is provided as part of a professional activity, it can be characterised as personal data.[134] It does not matter whether access to the information is limited

130 Regulation EU 2016/679.

131 *Opinion 4/2007 on the concept of personal data*, 2007.

132 See more extensively in Kokott and Sobotta, 2013.

133 C-615/13 P (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*), para. 32.

134 C-615/13 P (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*), para. 30.

or not. Therefore, in *Lindqvist* the CJEU considered that information published on a freely accessible webpage enjoys full protection under data protection law.[135] Regarding the concept of personal data, it does not matter whether the information is ordinary or sensitive, objective or subjective, true or false.[136] It can be stored in any medium or form. In its case law, the CJEU has interpreted the notion of personal data so broadly that it has thus far excluded only abstract legal analyses.[137]

The notion of "natural person" is straightforward since it always covers living natural persons.[138] Therefore, every time information relates to a living person, it is potentially that person's personal data. Crucial for determining whether something is personal data, especially in the context of the issues discussed in this chapter, is the notion of the relationship between the information and the person and the identifiability of that person. As mentioned, information is personal data if, among other conditions, it relates to a natural person. The criteria of "relationship" has so far been most developed by the Article 29 Working Party, which was established under Directive 95/46 as a body composed of a representative of the supervisory authority or authorities designated by each Member State. According to one opinion of this working party, the criterion of relationship requires that information be linked to a person based on its content, purpose, or results. The element of content is deemed to be satisfied if the information is very broadly "about a person". If this condition is not satisfied, it becomes relevant whether the information is processed with a purpose to 'evaluate, treat in a certain way or influence the status or behaviour of an individual'. Finally, if this is also not the case, then information can still be personal data if its processing 'is likely to have an impact on a certain person's rights and interests'. An impact does not have to be a major one, as it is sufficient that the individual may be treated differently from other persons as a result of the processing of the data.[139] The requirement that information relates to a person has not so far generated more extensive analysis by the CJEU, although the court did seem to endorse the criteria of the Article 29 Working Party when it concluded in *Nowak v. Data Protection Commissioner* that 'as regards the latter condition [relates to], it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person'.[140]

Finally, information related to a natural person is personal data if the person is identified or identifiable. This issue is subject to extensive debate,[141] as it has the potential to significantly impact the scope of the application of EU personal data

135 C-101/01 (*Lindqvist*), para. 27.
136 *Opinion 4/2007 on the concept of personal data*, 2007, pp. 6–9.
137 C-141/12 (*YS*), para. 39.
138 It is explained in Recital 27 of the GDPR that it does not apply to the personal data of deceased persons, but Member States may provide for rules regarding the processing of personal data of deceased persons.
139 *Opinion 4/2007 on the concept of personal data*, 2007, pp. 10–11.
140 C-434/16 (*Nowak v. Data Protection Commissioner*), para. 35.
141 Purtova, 2022.

protection rules. Many issues surround the notion of identifiability, but the key issue is what is actually meant by a person being "identified". To simplify a complicated issue to some degree, it might mean that a person's civil identity is determined, or, as was argued by Article 29 of the working party, that a person is somehow "distinguished" from all other members of the group.[142] But it appears that the CJEU did not follow the second approach in *Breyer v. Bundesrepublik Deutschland*, where it reasoned that an IP address 'does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer'.[143] Therefore, according to the CJEU, the question of whether a dynamic IP address is personal data depends on whether the owner of the address 'has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person'.[144] Based on this judgement, it appears that the court pursued the first approach mentioned above, which effectively requires establishing the data subject's civil identity. However, this approach is convincingly criticised in the legal literature, and there is also some guidance from national courts and data protection authorities which pursue different and broader interpretations of the element of identification.[145] Finally, on 7 March 2024 the CJEU published a decision in the *IAB Europe v. Gegevensbeschermingsautoriteit* case,[146] concluding that:

> a string composed of a combination of letters and characters … containing the preferences of a user of the internet or of an application relating to that user's consent to the processing of personal data concerning him or her by website or application providers as well as by brokers of such data and by advertising platforms constitutes personal data within the meaning of that provision in so far as, where those data may, by reasonable means, be associated with an identifier, such as, *inter alia*, the IP address of that user's device, they allow the data subject to be identified. In such circumstances, the fact that, without an external contribution, a sectoral organisation holding that string can neither access the data that are processed by its members under the rules which that organisation has established nor combine that string with other factors does not preclude that string from constituting personal data within the meaning of that provision.

While the CJEU still maintains that identifiability of the data requires the subject of the data to be "identified" (as opposed to singled out), the court did send a strong message that in the context of a particular case the string should be treated as personal data, since identification can happen on the basis of additional data, which

142 *Opinion 4/2007 on the concept of personal data*, 2007, p. 12.
143 C-582/14 (*Breyer v. Bundesrepublik Deutschland*), para. 38.
144 C-582/14 (*Breyer v. Bundesrepublik Deutschland*), para. 49.
145 See: Purtova, 2022.
146 C-604/22 (*IAB Europe v. Gegevensbeschermingsautoriteit*), para. 78.

do not necessarily have to be in the possession of the data controller. Finally, it is important to note that the court did not specifically mention its earlier position from *Breyer v. Bundesrepublik Deutschland*, pursuant to which it is relevant whether the data controller has the legal means to obtain the additional data necessary for identification (although this was one of the questions asked).

Looking from the perspective of the use of AI in the military and defence sectors to process data, the key initial challenge will be assessing whether certain data is "personal" in the sense of the GDPR. The problem here lies in the fact that the assessment of whether something is personal data involves complex case-by-case analyses in which multiple legal and technological issues need to be considered. The general issue, in our opinion, is that personal data is a much broader concept than one might think before making an appropriate analysis. Therefore, it might come as a surprise to many entities, including those in the military and defence sectors, to realise that the data they process are actually personal. For instance, when the NATO Data Exploitation Framework Policy mentions the 'protection of personally identifiable information and privacy', it is referring to concepts which are narrower than the personal data. As we have seen from the electronic communications cases, the CJEU is not shy about enforcing personal data protection rules to the fullest extent, even in cases which are ordinarily matters of national regulation.

Even if it is concluded that data is non-personal, it does not mean that it is outside the scope of EU law *per se*, since this matter is regulated by *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*.[147]

is the regulation on non-personal data contains a generic provision on its scope, pursuant to which it does not apply to an activity which falls outside the scope of Union law,[148] which, as explained in Recital 12, includes national security.

Compared to the GDPR, the aims of the Regulation on non-personal data are much more limited. Essentially this regulation aims to ensure the free flow of non-personal data within the Union by prohibiting data localisation requirements, thus ensuring the availability of data to competent authorities and facilitating the porting of data for professional users. The Regulation on non-personal data seeks to remove obstacles to the development of data economy in the Union, namely 'data localisation requirements put in place by Member States' authorities and vendor lock-in practices in the private sector'.[149] But the Regulation on non-personal data does not go further than that, and therefore, it will probably not have a significant impact on the use of data in the context of AI activities in military and defence sectors.

Next, we turn to the scope of application of the GDPR. According to Article 2(1), the GDPR applies to the processing of personal data wholly or partly by automated

147 Regulation (EU) 2018/1807.
148 Regulation (EU) 2018/1807, Article 2(3).
149 Regulation (EU) 2018/1807, Recital 2.

means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

As in the case of the ePrivacy Directive mentioned above, the GDPR also exempts some activities from its scope of application.[150] The issues discussed in this chapter include the processing of personal data in the course of an activity which falls outside the scope of EU law[151] and the processing of personal data by Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU.[152] As with other exceptions, the CJEU firmly holds that it must be interpreted narrowly.[153]

Recital 16 of the GDPR elaborates that the exemption for data processing activities outside the scope of EU law includes activities concerning national security. Notably, the earlier Directive 95/46 had the same exemption, specifying that it included 'processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) …'. Although the GDPR now refers only to national security purposes, there should be no doubt that activities outside the scope of EU law also includes data processing for national defence purposes. The CJEU considers the national security exemption a 'continuation of the first indent of Article 3(2) of Directive 95/46'. Therefore, the CJEU speaks about 'activity which is intended to safeguard national security or of an activity which can be classified in the same category'.[154] Moreover, the CJEU explicitly states that 'the activities having the aim of safeguarding national security … encompass… those that are intended to protect essential State functions and the fundamental interests of society'.[155]

Pursuant to the CJEU case law, there are two conditions which need to be satisfied cumulatively for an exception under Article 2(2)(a) to apply. These revolve around the identity of the data controller and the method of the data processing activity.

First, data processing activities should be carried out by competent authorities.[156] This seems, at least to some extent, supported by the reasoning of the CJEU in *La Quadrature du Net and Others v. Premier minister and Others*, where the court referred to Article 23 of the GDPR to differentiate between data processing activities carried out 'by competent authorities' as opposed to those carried out by individuals.

Secondly, it is not sufficient that data processing activity is 'characteristic of the State or of a public authority'.[157] Instead, it should be an activity genuinely intended

150 GDPR, Article 2(2).
151 GDPR, Article 2(2)(a).
152 GDPR, Article 2(2)(b).
153 C-439/19 (*B v. Latvijas Republikas Saeima*), para. 62; C-272/19 (*VQ v. Land Hessen*), C-311/18 (*Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*), para. 84.
154 C-439/19 (*B v. Latvijas Republikas Saeima*), para. 64.
155 C-439/19 (*B v. Latvijas Republikas Saeima*), para. 67.
156 C-439/19 (*B v. Latvijas Republikas Saeima*), para. 66.
157 C-439/19 (*B v. Latvijas Republikas Saeima*), para. 66.

to safeguard national security (or an activity which can be classified into the same category, e.g. national defence). As the CJEU explains, 'the activities having the aim of safeguarding national security that are envisaged in Article 2(2)(a) of the GDPR encompass, in particular, those that are intended to protect essential State functions and the fundamental interests of society'. Applying this standard, the CJEU concluded in 2022 that 'activities relating to the organisation of elections in a Member State do not pursue such an objective'.[158]

Overall, it does not seem likely that the use of personal data for purposes of AI in military and defence will be fully exempted from the scope of EU law. As a result, data protection rules, particularly the GDPR, will impact many aspects of data processing in these sectors. It will be necessary to comply with all personal data protection principles, including data minimisation, purpose limitation, and storage limitation. Specifically for purpose limitation, using data collected and processed by some private entities will be considered processing, and will require appropriate legal basis under national law. Finally, even when certain data processing activities fall outside the scope of EU law, they may still be subject to national constitutional law and the requirements of the ECHR.

4. Conclusions

The potential uses of AI in the military and defence sectors appear to be almost unlimited. As explained in this and other chapters, there is almost no area of military and defence activity in which AI could not make a meaningful impact. But to what extent is the development and use of AI in military and defence currently regulated in the EU? Our analysis shows that although there is no lack of regulation, the legal framework itself should not pose insurmountable obstacles for the industries and entities acting for the military and defence sectors. It seems likely that ethical considerations are the real factor preventing European countries from advancing more aggressively with AI solutions in the defence and military arenas.

This is visible for instance in the regulation of LAWS. While there are no binding EU rules on the matter, European institutions have strongly emphasised the responsible development and use of such systems. However, after careful consideration of the European Parliament's stance, it is evident that it is advocating for reasonable safeguards aimed at ensuring human control and accountability.

While autonomous drones and other lethal weapons systems acting without, or with limited human control, rightly occupy the top of the list of concerns, there are many more areas where AI can make a meaningful impact. Therefore, in this

158 C-306/21 (*Komisia za zashtita na lichnite danni and Tsentralna izbiratelna komisia v. Koalitsia Demokratichna Bulgaria – Obedinenie*), para. 41.

chapter, we examined the legal regulations for AI in general. We identified the forthcoming AI Act as the directly applicable EU regulation, but we also considered rules on access to data processed by AI systems.

The drafters of the AI Act made serious efforts to exclude the military, defence and national security sectors from the scope of application. However, this does not mean that all AI-related activities in these domains will avoid CJEU scrutiny. As the existing case law shows, the court has intervened in many cases in areas which are primary competencies of Member States, including matters of national defence. Therefore, it is possible that the same approach may also be followed in AI-related cases. In our view, considering the division of competences between Member States and the EU, the legislative history of the AI Act, and the challenges of regulating technologically advanced systems such as AI, it would be preferable to see the CJEU exercise its powers very cautiously when it inevitably faces questions about the use of AI in the military and defence domains.

Finally, we believe that the biggest challenges in the development and use of AI in the military and defence domains may stem from regulations governing data use. As data are what really fuels AI, access to data is of fundamental importance. Our analysis shows that current EU rules can be applied to the military and defence sectors, with fewer possibilities of exemption than in the AI Act, especially in light of existing CJEU case law. When we combine this with a broad concept of personal data, it is clear how personal data protection rules could seriously limit the ability of national defence and military entities to process certain types of data.

References

Anand, A., Deng, H. (2023) *Towards Responsible AI in Defence: A Mapping and Comparative Analysis of AI Principles Adopted by States*. Geneva: UNIDR.

Gosselin-Malo, E. (2023) 'NATO to update artificial intelligence strategy amid new threats', *Yahoo News*, 30 November 2023. [Online]. Available at: https://news.yahoo.com/nato-artificial-intelligence-strategy-amid-143228193.html (Accessed: 2 February 2024).

Gray, M., Ertan, A. (2021) *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment*. Tallinn: NATO CCDCOE.

Kokott, J., Sobotta, C. (2013) 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law*, 3(4), pp. 222–228; https://doi.org/10.1093/idpl/ipt017.

Nurkin, T. (2023) 'AI and Technological Convergence: Catalysts for Abounding National Security Risks in the Post-COVID-19 World' in Raska, M., Bitzinger, R.A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*. London: Routledge, pp. 37–58; https://doi.org/10.4324/9781003218326-3.

Purtova, N. (2022) 'From knowing by name to targeting: the meaning of identification under the GDPR', *International Data Privacy Law*, 12(3), pp. 163–183; https://doi.org/10.1093/idpl/ipac013.

Rickli, J.-M., Mantellassi, F. (2023) 'Artificial Intelligence in Warfare: Military Uses of AI and Their International Security Implications' in Raska, M., Bitzinger, R.A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*. London: Routledge, pp. 12–36; https://doi.org/10.4324/9781003218326-2.

Soare, S. (2023a) 'Algorithmic power? The role of artificial intelligence in European strategic autonomy' in Cristiano, F., Broeders, D., Delerue, F., Douzet, F., Géry, A. (eds.) *Artificial Intelligence and International Conflict in Cyberspace*. 1st edn. London: Routledge, pp. 77–108; https://doi.org/10.4324/9781003284093-6.

Soare, S. (2023b) 'European Military AI: Why Regional Approaches Are Lagging Behind' in Raska, M., Richard, B. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*. London and New York: Routledge, pp. 80–111; https://doi.org/10.4324/9781003218326-5.

Taddeo, M., Blanchard, A. (2021) *A Comparative Analysis of the Definitions of Autonomous Weapons Systems*. UNODA. [Online]. Available at: https://documents.unoda.org/wp-content/uploads/2021/10/20210721-Autonomous-Weapon-Systems-Definitions-TO-SHARE.pdf (Accessed: 30 October 2024).

Taddeo, M., McNeish, D., Blanchard, A., Edgar, E. (2023) 'Ethical principles for artificial intelligence in the defence domain' in Cristiano, F., Broeders, D., Delerue, F., Douzet, F., Géry, A. (eds.) *Artificial Intelligence and International Conflict in Cyberspace*. 1st edn. London: Routledge, pp. 159–185; https://doi.org/10.4324/9781003284093-10.

Géry, A. (ed.) *Artificial Intelligence and International Conflict in Cyberspace*. 1st edn. London: Routledge, pp. 160–185; https://doi.org/10.4324/9781003284093-10.

Unauthorized use of cellphones by Russian soldiers led to Ukrainian strike that killed 89 troops, military says (2023) *CBS news*, 4 January 2023. [Online]. Available at: https://www.cbsnews.com/news/ukraine-news-russia-military-blames-cell-phones-strike-soldier-deaths/ (Accessed: 30 October 2024).

Policy documents

Devitt, K., Gan, M., Scholz, J, Bolia, R. (2020) *A Method for Ethical AI in Defence*. Canberra: Australian Department of Defence. [Online]. Available at: https://www.dst.defence.gov.au/sites/default/files/publications/documents/A%20Method%20for%20Ethical%20AI%20in%20Defence.pdf (Accessed: 30 October 2024).

Digitalization and Artificial Intelligence in Defence (2019) *Food for Thought Paper by Finland, Estonia, France, Germany, and the Netherlands*, 15 May. [Online]. Available at: https://valtioneuvosto.fi/documents/11707387/12748699/Digitalization+and+AI+in+Defence.pdf/151e10fd-c004-c0ca-d86b-07c35b55b9cc/Digitalization+and+AI+in+Defence.pdf (Accessed: 30 October 2024).

European Commission (2018) 'Artificial Intelligence for Europe', COM/2018/237 final, *EU Monitor*, Brussels, 25 April.

European Commission (2019) 'Ethics Guidelines for Trustworthy AI', *High-Level Expert Group*, 8 April. [Online]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (Accessed: 30 October 2024).

European Commission (2020) 'White Paper On Artificial Intelligence – A European approach to excellence and trust', COM(2020) 65 final, Brussels, 19 February.

European Parliament (2014) *Resolution of 27 February 2014 on the use of armed drones*. OJ C 285, 29 August 2017, pp. 110–111.

European Parliament (2018) *Resolution of 12 September 2018 on autonomous weapon systems*, OJ C 433, 23 December 2019, pp. 86–88.

European Parliament (2020) *Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, OJ C 404, 6 October 2021, pp. 63–106.

European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (2021) COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), Brussels, 21 April 2021. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7536_2024_INIT (Accessed: 30 October 2024).

European Union External Action (2022) *A Strategic Compass for Security and Defence*. [Online]. Available at: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf (Accessed: 30 October 2024).

French Ministry of Defence (2019) 'Artificial Intelligence is Support of Defence', September 2019. [Online]. Available at: https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf (Accessed: 30 October 2024).

NATO (2021a) 'Summary of the NATO Artificial Intelligence Strategy', 22 October 2021. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_187617.htm (Accessed: 30 October 2024).

NATO (2021b) 'Summary of NATO's Data Exploitation Framework Policy', 22 October 2021. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_210002.htm (Accessed: 30 October 2024).

UK Ministry of Defence (2022) 'Defence Artificial Intelligence Strategy', June 2022. [Online]. https://assets.publishing.service.gov.uk/media/62a7543ee90e070396c9f7d2/Defence_Artificial_Intelligence_Strategy.pdf (Accessed: 30 October 2024).

US Department of Defense (2019) *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity.* [Online]. Available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (Accessed: 18 January 2024).

Legislation, international treaties and guidelines

Convention on Cybercrime (2001) ETS 185, Budapest, 23 November 2001.

Council of Europe (2001) 'Explanatory Report to the Convention on Cybercrime', ETS 185, Budapest, 23 November.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002) OJ L 201, Brussels, 31 July 2002, pp. 37–47.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (2006) OJ L 105, 13 April 2006, pp. 54–63.

Opinion 4/2007 on the concept of personal data (2007) Article 29 Working Party Archives 1997 – 2016. [Online]. Available at: https://ec.europa.eu/justice/article-29/documentation (Accessed: 30 October 2024).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (2021) COM(2021) 206 final, Brussels, 21 April 2021. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A0206%3AFIN (Accessed: 30 October 2024).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (2021) 2021/0106(COD), Brussels, 29 November 2021. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf (Accessed: 30 October 2024).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 119, 4 May 2016, pp. 1–88.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (2018) OJ L 303, 28 November 2018, pp. 59–68.

Case-law

Court of Justice of the European Union, C-101/01 (*Lindqvist*).

Court of Justice of the European Union, C-141/12 (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*).

Court of Justice of the European Union, C-186/01 (*Dory v. Bundesrepublik Deutschland*).

Court of Justice of the European Union, C-273/97 (*Sirdar v. The Army Board and Secretary of State for Defence*).

Court of Justice of the European Union, C-285/98 (*Kreil v. Bundesrepublik Deutschland*).

Court of Justice of the European Union, C-306/21 (*Komisia za zashtita na lichnite danni and Tsentralna izbiratelna komisia v. Koalitsia „Demokratichna Bulgaria – Obedinenie”*).
Court of Justice of the European Union, C-203/15 and C-698/15 (*Tele 2and Watson v. Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*).
Court of Justice of the European Union, C-272/19 (*VQ v. Land Hessen*).
Court of Justice of the European Union, C-311/18 (*Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*).
Court of Justice of the European Union, C-434/16 (*Nowak v. Data Protection Commissioner*).
Court of Justice of the European Union, C-439/19 (*B v. Latvijas Republikas Saeima*).
Court of Justice of the European Union, C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others v. Premier minister and Others*).
Court of Justice of the European Union, C-582/14 (*Breyer v. Bundesrepublik Deutschland*).
Court of Justice of the European Union, C-604/22 (*IAB Europe v. Gegevensbeschermingsautoriteit*).
Court of Justice of the European Union, C-615/13 P (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*).
Court of Justice of the European Union, C-742/19 (*B.K. v. Republika Slovenija*).

IV.3

MILITARY AND DEFENCE ISSUES IN SPACE

Chapter 10

Challenges of Practical Space Operations Under the Outer Space Treaty: Operations in a Legal Regime of a Different Era

Attila Horváth

Abstract

Outer space is of the utmost importance for our society. It is endless, but still limited. It is used to support activities related to business, state, and defence, and while it is replaceable, this replacement would negatively affect our way of life. Its importance also creates a vulnerability that can be exploited by adversaries, however, pure chance can trigger events that can lead to catastrophes. Outer space is, by its very nature, an international environment. Still, the international legal regime regulating it is surprisingly limited compared to its vital importance. This chapter presents several examples wherein the regulations have fallen behind the advance of technology and operations. These shortcomings did not come to light until now only because of practical technology's inability to realise what is theoretically possible, professionalism of the operators, and sheer luck. It would be unwise to count on these reasons in the future. This chapter organises the examples into the following groups: delimitation of airspace and outer space and operations in the border region; sovereignty and zoning of outer space related to spacecraft; operations of active spacecraft and removal of inactive ones; and defence-related technology development. At the end of each section, questions and suggestions are presented for the legal community to examine and discuss. It is my desire to use this opportunity to support the legislative effort necessary to develop legally binding and enforceable rules and

Attila Horváth (2024) 'Challenges of Practical Space Operations Under the Outer Space Treaty: Operations in a Legal Regime of a Different Era'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 437–477. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_10

regulations, so as to enable the sustainable long-term use of outer space – a natural resource incomparable to any other.

Keywords: spacecraft, Outer Space Treaty, delimitation, sovereignty, dual-use, mesosphere, space debris

1. Introduction

Outer space is a special realm, both physically and legally. Most of our understanding about the earth's environment – just like our earthly laws and rules of behaviour – can be applied to space only with extreme caution. The legal regime of outer space was established decades ago, when the utilisation of outer space was very different. At that time, the actors executing space activities were state agencies, including military forces and national security organisations. Commercial space activities were envisioned, but were understood as state controlled. Most of the space operations were related to exploration and support of state functions, including the provisioning of public services and the support of security and military operations. The small number of spacefaring nations and the limited scope of activities suggested that a limited set of rules would be enough, since these were based on a common understanding and mutual cooperation.

It soon became apparent that this would not be the case. Two significant examples can be recalled (among many more) to illustrate the fragility of the space treaties, even at that time. The first example is the case of the Soviet spacecraft Kosmos[1] 482. Kosmos 482 was launched on 31 March 1972 from Baikonur Cosmodrome, on a launch vehicle generally used to launch the Venera series space probes, onto a trajectory typical as a parking orbit for interplanetary missions.[2] However, the upper stage suffered a malfunction, and the space vehicle separated into multiple pieces. At least one object (international designation 1972-023E, most likely the Venus descent module) is still in orbit. One object reentered just a day after launch (1972-023B, launch vehicle second stage), another (1972-023A, main spacecraft module) reentered in 1981, and a further one (1972-023D, launch vehicle third stage) reentered in 1983 without any incident. However, object 1972-023C, an intermediate stabilising platform used for interplanetary launches onboard Molniya launch vehicles, re-entered on 2 April 1972.[3] During reentry, the object disintegrated, and

1 The name "Kosmos" was used by the Soviet Union, and is still used by Russia, to designate classified, unspecified, or failed space missions. Usually, Kosmos spacecraft were announced with cover stories of unspecified, but usually technological or scientific, research missions.

2 Langbroek, 2022.

3 Zak, 2011.

four spherical tanks made of titanium reached the surface in New Zealand, causing negligible property damage.

The tanks were marked with Russian markings and were identified as objects from the Kosmos 482 launch; therefore, the New Zealand government contacted the Soviet Union to return the debris. However, the Soviet Union denied ownership, and the case came to a dead end.

The second example of the fragility of the space legal regime is the case of the Bogotá Declaration.[4] The Bogotá Declaration was issued by eight countries located along the equator, which asserted their sovereignty over sections of the geostationary orbit[5] while leaving other volumes of outer space as the common heritage of mankind, as described in the Outer Space Treaty.

The argument behind the assertation was that the geostationary orbit is a consequence of the gravity and rotation of the Earth; therefore, this orbit is not simply a location in outer space but rather a natural resource directly linked to the territory of the country at the subsatellite point.

The Bogotá Declaration reiterated the missing definition of outer space in the Outer Space Treaty of 1967.[6] It referenced Resolutions 2692[7] and 3281[8] of the United Nations (UN) General Assembly.[9] Altogether, the declaration presented an argument stating that since geostationary orbit is possible because of Earth's gravity, and Earth's gravity is a consequence of Earth's mass, the sovereignty over a given Earth's mass is granted by the UN resolutions, and outer space is not defined internationally; therefore, sovereignty over sections of the geostationary orbit can be established.

Ultimately, the Bogotá Declaration failed to gain any significant international support outside the eight nations. However, loopholes exploited by the declaration still have not been closed by international laws.

The advancement of technology and proliferation of space activities created and, in my opinion, continue to create many similar problematic cases. In this chapter, I plan to outline a selection of these cases and call for the legal community to create universally accepted legal controls to enable safe and effective space operations, as well as prevent any possible conflicts (including legal and physical).

This chapter will present cases according to the following structure:

4 Durrani, 2017.

5 The geostationary orbit is a subset of the geosynchronous orbits around the Earth. The time an object on a geosynchronous orbit requires to orbit the Earth precisely equals the time the Earth needs to complete one rotation. When the orbital plane coincides with the equatorial plane, the object orbits without any relative motion in reference to an observer located on the surface of the Earth (no East-West and no North-South relative motion).

6 UN General Assembly, 1967.

7 UN General Assembly, 1970.

8 UN General Assembly, 1974.

9 These resolutions confirmed the sovereignty of states over their natural resources.

An important question regarding the legal status of space operations is the delimitation of the atmosphere (where state sovereignty is in effect) and outer space (where sovereignty is out of the question). Section 2 examines cases where the lack of uniform and internationally accepted delimitation between the atmosphere and outer space hinders the development or execution of space activities. Selected examples for this section include the following:

- Hypersonic flights in the mesosphere
- Suborbital spaceflight
- Flights where different sections use different principles of flight – alternating between Keplerian or suborbital trajectories and atmospheric aerodynamic (hypersonic) flight

There is also a question of sovereignty in outer space. According to the existing legal regime, state sovereignty ends at the outer extremes of a spacecraft body, but safe and effective space operations require separation of spacecraft in orbit. Section 3 presents arguments why there needs to be a volume around each spacecraft that effectively belongs to said spacecraft because of the uncertainties of the tracking and manoeuvring systems. Selected examples for this section include the following:

- Legality and enforceability of the existing keepout zones used voluntarily in international space activities (International Space Station [ISS] operations and the Artemis Accords)
- Legal status of non-cooperative rendezvous and proximity operations (close approach and formation flying by a spacecraft with another spacecraft)
- Legality of the enforcement of unilaterally declared security zones (patrol spacecraft)

Next, in Section 4, I discuss the definition of operational spacecraft as well as responsibilities of spacecraft operators during and after the useful operational life of a spacecraft (closely related to damages). Selected examples for this section include the following:

- Lack of definition of an operational spacecraft and the valuation of an inoperational spacecraft
- Orbital debris removal by third parties or as a public service
- Chain-event effects and indirect damages

Next, in Section 5, I discuss the regulation of legal self-defence technologies with offensive applications, dual-use technologies, and weaponisable commercial space technologies. Selected examples for this section include the following:

- Orbital debris removal (weaponisable as a co-orbital counterspace weapon)
- Ballistic missile defence (legal self-defence capability that can be used as a direct-ascent counterspace weapon)
- Directed energy jammers

2. Questions Arising from the Lack of Delimitation of Airspace and Outer Space

There is no internationally accepted general definition of outer space, spacecraft, space activity, or the boundary between the sovereign airspace and outer space. Sovereign states have their defined responsibilities in their airspace (e.g. see Chapter 1 of the Convention on International Civil Aviation). Simultaneously, because of the Outer Space Treaty, there is no sovereignty in outer space. There needs to be a line where these rules and the associated responsibilities change based on different situations.

While there are no defined rules for delimitation, there exist dozens of theories for it. These can be grouped into two main categories: spatial delimitation and functional delimitation theories. However, neither of these can provide a universal answer.[10]

Spatial delimitation theories arbitrarily select either an altitude or a physical phenomenon to calculate an altitude, the volume below which is part of the airspace and above which is part of outer space. The limit most often mentioned is the Kármán line (as an arbitrarily selected physical phenomenon); however, the actual altitude (100 km above main sea level) does not correspond to the Kármán line[11] and so is also an arbitrarily selected altitude.

Functionalist delimitation theories focus on the activity itself and not its physical location. Practically, functionalist delimitation theories can be summarized as stating that an object that does space activities is in outer space. However, since space activities are not defined in international law, this approach again calls for arbitrarily selected activities based on the definition. For example, if the arbitrarily selected criterion is completing an orbit around Earth, an experimental, very low Earth orbit[12] satellite that orbits (for a very limited time) on a 180-km circular orbit can be defined as a spacecraft and therefore as being in outer space; however, the target vehicle of an antiballistic missile test that reaches an altitude of several thousand kilometres on a suborbital trajectory does not fall under this definition.

This lack of internationally accepted legal definition makes it difficult to even write about the problem itself – How to differentiate between spaceflight and atmospheric

10 Bartóki-Gönczy and Sipos, 2022.

11 The Kármán line is based on the fact that the diminishing atmosphere can only provide enough lift for aerodynamic flight if the airspeed is increasing. When the required airspeed reaches the first orbital speed, the need for lift disappears, since from here on the object is not flying aerodynamically but is on a Keplerian orbit. The Kármán line is not constant but can be calculated to lie around 85–90 km, depending on the density of the upper atmosphere. The problem with this theory is that there are practical atmospheric effects (drag and chemical interactions) above this altitude, while sustained orbital operations are not possible here. For a detailed analysis of the Kármán line, see: McDowell, 2018.

12 Laursen, 2023.

flight if we do not know where space is and what is spaceflight? Therefore, this chapter also uses the expression "exoatmospheric flight" to describe flights where physical effects other than aerostatics or aerodynamics dominate flight dynamics.

2.1. Hypersonic Mesospheric Flight

The mesosphere is the layer of the Earth's atmosphere lying above the stratopause and below the mesopause, roughly between 50 km and 80–90 km (varying, depending on the geographical location and upper atmospheric weather). The most important property of the mesosphere (and which is used to define it) is that the temperature decreases with altitude.[13]

The mesosphere cannot be reached with conventional aerodynamic aircrafts and is practically unreachable for aerostatic balloons (although it is not impossible for special balloons made of ultralight materials to reach it). Sustained (straight and level) aerodynamic flight is only possible at hypersonic velocities.

Hypersonic flight is usually defined as supersonic flight above Mach 5.[14] Practically, however, hypersonic flight is usually associated with rocket- or scramjet-[15]powered aerodynamic vehicles (capable of sustained straight and level flight) and hypersonic gliders that convert their potential energy to kinetic energy to achieve limited manoeuvring and flight time. Hypersonic gliders are usually launched with rocket power, including military ballistic missiles (hypersonic warheads such as the Russian Avangard[16] or the discontinued US AMaRV[17]), modified space launchers (RocketLab Electron HASTE[18]), and suborbital launch vehicles.

One significant physical phenomenon associated with hypersonic flight is the heat transfer between the vehicle and the surrounding air. This limits the practical hypersonic flight to altitudes where the air density is relatively low (to reduce heating) but still sufficient to generate lift. This practically coincides with the mesosphere.

As of today, there are very limited commercial activities, and somewhat more research activities, related to hypersonic flights. Nevertheless, there are military applications of this flight regime, mostly involving weapons delivery and missile defence. The commercial applications are expected to be developed with the advancement of technology, mostly in transportation.

The mesosphere and hypersonic flights are in a grey zone. The physical domain is inside the atmosphere, and the flight is based on the interaction with the air. However, this domain is unreachable for most of the air defence systems used by

13 For a short description of the mesosphere, see: University of Wuppertal, no date.
14 Brockmann and Schiller, 2022.
15 Scramjet is short for supersonic combustion ramjet, an air-breathing thermal engine without moving parts in which the combustion that generates the thrust occurs in a supersonic airflow environment. For a short description of scramjets, see: SKYbrary, no date.
16 Missilethreat, 2021.
17 Bunn, 1984.
18 Rocketlab, no date.

militaries, and it is even above the detection threshold of most unmodified air surveillance radars. Therefore, practical enforcement of state sovereignty is questionable. This is an important point, since the basis of sovereignty over the seas originally arose from the ability of a coastal nation to defend its shores with military power (coastal defence artillery).[19]

The technology used to reach the mesosphere and perform flight operations there is closely related to space technology. Thermal protection of the vehicle needs to be comparable to the thermal protection used in spacecraft reentry, as the speeds and altitudes are also comparable. Scramjet propulsion is exclusively an aerial system, but rocket propulsion used in hypersonics is again directly comparable to space technology. Moreover, a rocket-powered hypersonic vehicle is capable of flight only slightly above the most often cited boundary of airspace and outer space, with its operational radius limited only by its onboard fuel. Therefore it is theoretically possible to complete a circumnavigation of Earth at an altitude of, for example, 110 km, with a hypersonic lift vehicle (which in this case might fall under the definition of spacecraft by either the functionalist or spatial delimitation); at the same time, a similar vehicle can complete the circumnavigation with exactly the same technology and operational rules at 90 km, or just execute an intercontinental transfer at these altitudes (or even lower). It must be noted that such circumnavigation is possible at velocities lower than the corresponding orbital velocity, using any aerodynamic lift still present, but mostly engine thrust to counteract gravity.

Third, a hypersonic glider can start its flight as a suborbital or even orbital spacecraft. Since a hypersonic glide is a manoeuvre converting potential energy to kinetic energy, the vehicle needs to reach a certain altitude and then start falling back towards the Earth (executing a reentry from space or simply starting an unpowered, almost horizontal flight in the atmosphere). During the glide, the vehicle uses its aerodynamic surfaces to generate lift and steering forces; meanwhile, the associated drag slows it down. To avoid losing its kinetic energy, the vehicle must lower its altitude. Ultimately, the combined energy will be reduced below a certain level where the hypersonic flight is finished (because the vehicle either slows down or hits the surface). This set of manoeuvres is comparable to a controlled reentry from outer space; however, it is questionable whether the rules concerning reentry are applicable in this case, since the ascent to outer space itself was only executed to provide the initial potential energy.[20]

19 Pogies, 2021.

20 In the case of a hypersonic glide starting with sustained orbital spaceflight, the orbits are typically used for prepositioning the vehicle to the appropriate position in space and time for a successful hypersonic flight.

2.2. Suborbital Spaceflight

The core challenge with suborbital spaceflight is that it is easy to misunderstand. The "sub" part of the word suggests that suborbital flights are happening below the orbital regime, but this is not necessarily true. Suborbital flights do not complete a full orbit around the Earth. There can be several reasons for this.

First, it is possible that the flight does not reach an altitude where sustained orbital flight is possible (in which case, the flight is very much comparable to the mesospheric flights described in Section 2.1.). Second, it is possible that that the vehicle does not have enough kinetic energy to complete the orbit (the scalar value of actual vehicle velocity is below the scalar value of orbital velocity of the respective trajectory), even if it reaches altitudes where orbiting spacecraft usually operate. This is the situation during, for example, military intercontinental ballistic missile launches. Third, even if the scalar value of actual vehicle velocity is over the orbital velocity, and the combined energy of the vehicle is enough for orbiting, the vehicle cannot complete an orbit if the actual velocity vector points in a direction that is inconsistent with orbiting (an extreme example is the directly vertical direction during the active part of the launch). Potential examples for this trajectory include scientific launches into the Van Allen Belts (to record a vertical cross-section of the radiation environment) or direct-ascent antisatellite weapons against medium (or higher) Earth orbit satellites.

Currently, suborbital flights are usually used for scientific research, technology development, military (ballistic missiles, ballistic missile defence, and antisatellite weapons), and commercial purposes, including human suborbital flights reaching over 100 km (Virgin Orbit and Blue Origin). Nonmilitary flights usually start and end in the same country or in international waters.

However, there is an emerging application of point-to-point transportation of goods and people (e.g. the SpaceX Starship P2P,[21] also known as Starport Network). During a suborbital point-to-point delivery flight, the vehicle launches onto a ballistic trajectory, leaves the dense atmosphere, transits the volume where spacecraft typically operate, reenters the dense atmosphere, and lands (practically, the same trajectory on which military intercontinental ballistic missiles fly). During this flight, the vehicle is expected to fly over the territory of more than one country. The trajectory transects the air volume typically used by not only conventional aircrafts but also orbiting spacecrafts. However, it is not clear whether the atmospheric flight sections correspond legally to space launch and re-entry (although technically they do) and whether the high-altitude coast corresponds legally to spaceflight (although technically it does).

Practically, it is possible to complete a suborbital flight by launching from international waters or airspace, transiting over countries above the dense atmosphere, and then re-entering over international waters. Such a flight would be completely

21 Wilken and Callsen, 2023.

outside sovereign national control if the exoatmospheric flight section is considered spaceflight. While international controls do exist,[22] there are no enforcement mechanisms related to these controls.

However, if the exoatmospheric flight is not considered spaceflight (e.g. if the delimitation is based on a functionalist approach requiring completed orbit), this flight again falls under the Chicago Convention, but without any practical means for the state to execute its sovereign rights (e.g. Article 10 of the Chicago Convention[23] established a right for states to require the landing of overflying aircraft at a designated customs airport, which would be practically impossible in the case of a suborbital vehicle).

2.3. Flights that Alternate between Different Flight Regimes

The combination of orbital or suborbital exoatmospheric flight and endoatmospheric aerodynamic flight is not new. It was proposed by Eugen Sänger and Irene Bredt, engineers working in Germany in the 1930s. Their system, called Silbervogel,[24] was based on a hybrid winged and lifting body airframe that launches on a suborbital energy trajectory and reaches altitudes between 100 and 200 km (several trajectories were computed by the designers, and the mentioned values can be found for flights with intercontinental reach and practical payload weights). Then, the vehicle starts its descent; in the denser atmosphere, it uses its lift-generating surfaces to achieve a positive climb again (sacrificing kinetic energy), and it starts another climb but with a lower maximum altitude. Ultimately, the vehicle reaches its destination with several hops, each lower and shorter than the previous. With enough initial energy, the vehicle is computed to be able to circumnavigate Earth.

Many similar designs were developed in the decades following the Second World War, in both the Soviet Union and United States (US). Generally, these designs are called boost-glide vehicles. All those utilising these vehicles fell victim to their lack of necessary technology required, but they also lacked any appropriate business case or military operational need.

Similar principles were considered during the Apollo lunar programme for use during atmospheric reentry from the direct trans-Earth trajectory from the Moon (called skip reentry). Ultimately, while skip reentry became unnecessary, it was used during the design of the Orion spacecraft and the Artemis programme's lunar return trajectory design to limit the heat load on the capsule's thermal protection system. Skip reentry was also used by the Soviet and Chinese Moon probe returns to enable increased manoeuvrability during reentry.

All the previously designed or flown boost-glide or skip reentry vehicles were unpowered after the initial launch or (in the case of lunar spacecraft) after trans-Earth

22 Sipos, 2018.
23 ICAO, 2006, p. 6.
24 Sänger and Bredt, 1944.

injection. However, it is not impossible to combine the boost-glide trajectory with rocket or scramjet propulsion, thereby combining the previously mentioned hypersonic lift vehicles with the boost-glide principle. Such a vehicle would launch on a rocket, reach exoatmospheric altitudes, and coast (or even orbit) there. Descending into the denser atmosphere, it would use atmospheric lift to increase its altitude (potential energy) and use its engines to replenish the kinetic energy lost during the climb.

To effectively coast between the climb sections, the vehicle needs to reach an altitude of at least 130–150 km to minimise drag, or even the altitude usually occupied by orbiting spacecraft. However, to generate enough lift and operate the scramjet engines (scramjets are air-breathing), it needs to descend deep into the mesosphere. Note that during the lift sections, the lift vector can be oriented to the left or right of the flight path, to enable steering (this manoeuvre is routinely used during spacecraft reentry).

By combining the technical questions of mesospheric hypersonic flight and suborbital exoatmospheric flight, this technology effectively combines the legal problems as well. The boost-glide vehicle can circumnavigate Earth, but this is not a Keplerian orbit. It reaches altitudes usually associated with spaceflight but spends a significant amount of time in the denser atmosphere (mesosphere) too. It transits the airspace used by conventional aircraft and by launching or re-entering spacecraft, but these transits are not space launches or re-entries. Finally, by using engine thrust and manipulation of the lift vector, the boost-glide vehicle can execute manoeuvres impossible for spacecraft, and while it uses the denser atmosphere for this, it cannot land at will at the usual airports to comply with the orders of national authorities for inspection and customs procedures.

2.4. Section Summary

In this section, I introduced three emerging and potentially disruptive technologies that ride, both physically and legally, the imaginary fence between airspace and outer space.

The three technologies – hypersonic flights in the mesosphere, suborbital point-to-point flights over long distances, and boost-glide flights – share some common questions about the lack of legal controls:

- They are not spaceflights as it is commonly understood; however, they reach altitudes outside the denser atmosphere usually associated with spaceflight and used by orbiting spacecraft.
- A significant amount of the flights' operational time is spent in the mesosphere, a region that is usually not considered as outer space; however, their interaction with the atmosphere is different from the way conventional aircraft interact with the atmosphere. These atmospheric flight sections are not space launches or re-entries. The vehicles are physically incapable of

complying with the rules set in Article 10 of the Chicago Convention, while at the same time, the states are usually incapable of enforcing compliance.
– When the necessary technology is developed (mainly scramjet propulsion and structural and thermal protection materials), these vehicles will be capable of alternating between endoatmospheric and exoatmospheric flight without entering orbit or finishing their flight in the denser atmosphere.

The lack of commonly understood and legally binding delimitation of airspace from outer space makes it impossible to develop operational rules, regulations, and guidelines for these technologies. As demonstrated earlier, it is possible to execute such flight operations by completely staying out of national controls. Moreover, with the proliferation and commercialisation of space and space-related technologies, manufacturers and operators are practically capable of performing these flight operations, and their compliance (in extreme cases) will be expected to be strictly voluntary.

It is desired that the international legal community, in cooperation with the manufacturers and operators, develops rules and regulations concerning these technologies. It is also recommended that these regulations create an intermediate zone above the volume where conventional air operations occur and below the volume where conventional space operations occur. There are initiatives for a similar zone in the stratosphere to regulate the traffic of high-altitude platform stations (stratospheric aerostatic and aerodynamic aircraft) above the volume used by conventional air traffic. This zone is planned to be based on physical delimitation, at a preset altitude around flight level 550 or 600 (roughly 17 km above the main sea level).[25] Similarly, a preset altitude can be selected, possibly around 150 km, to serve as the upper limit. This altitude is based on McDowell's[26] recommendation of 125 km (lower limit of sustained circular orbits), but it is extended upwards to account for the dynamic nature of the upper atmosphere. Similar volumes have already been advocated for, and J.N. Pelton's[27] proposal of the proto-zone[28] between 21 and 160 km is widely discussed but is, of course, not codified. From the operational point of view, such a designated intermediate volume would be beneficial.

It is also necessary that, following the establishment of the intermediate zone, an international convention develops a set of rules – which are comparable to the Chicago Convention and its relevant annexes (about the rules of flight operations in international airspace) – about operations in this new intermediate zone and the interaction with the airspace below and outer space above.

Defence-related applications of these technologies include weapons delivery, reconnaissance, and transportation of troops and supplies. All of these can be

25 EASA, 2023.
26 McDowell, 2018.
27 Pelton, 2016.
28 Alternative spelling: protozone.

very sensitive issues in international relations. This underlines the necessity of legislation.

3. Questions of the Sovereignty in Outer Space

The Outer Space Treaty clearly mentions that state sovereignty cannot be applied to any volume of outer space (Article II); at the same time, it specifies that states are responsible for the operation of their spacecraft (Article VIII). These two rules combined dictate that state sovereignty applies to the outside parts of the spacecraft, and ends there. Outside the physical body of the spacecraft, the volume of outer space is free for exploration and use.

Orbital mechanics dictate that spacecraft in orbit are moving. This practically means that the orbiting spacecraft occupies a given volume for an infinitely short amount of time; then it moves on, and the previously occupied volume is available again for free use by other space actors. It is the responsibility of spacecraft operators to ensure that no two spacecraft occupy the same volume at the same time (which would mean a collision).

Practical considerations related to space surveillance, spacecraft tracking, and navigation make this theoretical situation somewhat unclear. Spacecraft are not tracked with absolute certainty, and there are always errors in the measurements and predictions; therefore, operators consider elliptical volumes around their respective spacecraft as the basis of collision-avoidance manoeuvres.[29] The size of the elliptical volume directly depends on errors in the measurements, and it is generally accepted that these volumes are not "occupied" by the spacecraft and are subject to change according to the sensor properties and the advance of technology. However, this can cause misunderstandings when two operators, working with orbital element sets with different error levels, disagree on the probability of a potential collision and the necessary avoidance manoeuvres. Therefore, only a universal space traffic control system can provide adequate general answers to this problem.

3.1. Limited-Use Zones in Space Operations

In addition to the aforementioned virtual volumes, there exist (or are planned to exist) zones around spacecraft that are physical reality and are (planned to be) used to control the interaction of spacecraft. One example is the set of approach rules to

29 During rendezvous and proximity operations, where absolute certainty is necessary, onboard sensors are used for more precise measurements and manoeuvre planning.

the ISS,[30] the other is the safety zone concept described in the Artemis Accords.[31] We can safely assume that with the proliferation of human presence in Earth orbit and cislunar space and the advancement of uncrewed space vehicle approach and manoeuvring technologies, many more similar rules about operational safety zones (as they can be collectively called for practicality) will be written. These rules describe the procedures and limitations to be observed during approach to the respective space objects. However, these are not universal regulations, but commonly agreed rules binding only the respective parties. Noncompliance with these rules is to be dealt with by the parties to the agreements.

It is unclear, however, how the breach of such an operational safety zone by an outside actor can be dealt with. For a theoretical case study, let us assume that a highly agile and manoeuvrable spacecraft of an identified operator that is not a party to the ISS agreements and memorandums enters the operational safety zone around the ISS. This spacecraft is under continuous control of its operator, was not identified as a collision risk before the approach manoeuvre (because of which ISS did not execute collision-avoidance manoeuvres), and is keeping a stable distance from the ISS after entry into the zone without posing any direct risk. However, its presence still disrupts the ongoing operations of the station.

It is clear that the agreements defining the operational safety zone do not apply to the operator of the intruding spacecraft. This operator would declare that, under the Outer Space Treaty, the manoeuvre was an innocent free use of outer space, and that the spacecraft was capable of safely operating in close proximity to ISS and not causing any harm. The same case can be applied to an intrusion into the safety zone around a lunar installation of a party to the Artemis Accords by an outside actor.

Since the case reaches a dead end here under the Outer Space Treaty, there is a risk of creating a "new normal" when such intrusions continue. Diplomatic actions and international pressure can (and surely would) be applied to mitigate the situation. However, in my opinion, under the current international space legal framework, further sanctions are not possible.

3.2. Noncooperative Rendezvous and Proximity Operations

This case is a generalisation of the previous one. Operational safety zones are defined according to the current best understanding and best practices related to orbital operations, and they are specific to the respective few spacecraft or, in the case of the Artemis Accords, lunar installations. However, with the advancement of technology, noncooperative approaches to rendezvous and to fly in formation with any spacecraft are currently possible or will be in the near future. Even if such an

30 The approach procedures are described in detail in the 'ISS COTS Interface Requirements Document SSP50808', which is controlled by the International Traffic in Arms Regulations (ITAR). For an excerpt that falls outside ITAR controls, see: DuPont, 2005.

31 Schingler, 2020.

approach does not end with contact or collision, it can still disrupt the normal operation of the target spacecraft.

There are several reasons related to military or national security activities for why an uncooperative rendezvous and proximity operation might be beneficial from the point of view of the operator of the approaching spacecraft. The clearest reason is to preposition a kinetic antisatellite weapon[32] for a strike with a relatively short timeline. However, a close approach can enable electronic warfare (signal intelligence or jamming) activities with different attack geometries from those executed from the surface;[33] it also enables close inspection of the spacecraft with various sensors[34] and harassment.

At the same time, there are (or planned to be) numerous peaceful applications for this technology. The most well-known are space station resupply (and by extension, logistics related to uncrewed in-space manufacturing stations), orbital servicing (operational lifetime extension),[35] space debris removal,[36] and in-space construction.

The operator of the target spacecraft can only blindly trust that the approaching spacecraft is capable of safely executing the approach, rendezvous, and proximity operations, and that the operator of the approaching spacecraft does not have harmful intent. Therefore, the operator of the target spacecraft can utilise one of the following measures:

- Do nothing. However, in this case, the target spacecraft becomes a sitting duck.
- Perform preventive avoidance manoeuvres. In this case, operations of the target spacecraft get disrupted, and its operational life is shortened because of the unplanned spending of fuel.
- Call for public attention and the application of soft power. In this case, the operator of the approaching spacecraft can assert that the approach is simply an innocent free use of outer space and portray themselves as victims.
- Execute active measures to prevent the approach. In this case, the operator of the target spacecraft becomes the aggressor, since the approaching spacecraft has not yet performed anything that is harmful and not a free use under the Outer Space Treaty.

Altogether, the main problem with this current unregulated situation is that these "tailgating" operations can create a "new normal" where deviation from the previously understood (unwritten) behaviours become accepted just because they are performed many times. Successful rendezvous and proximity operations had already

32 A historical example is the Soviet IS antisatellite weapon system. For a description, see: Zak, 2024.
33 A historical example is the US electronic intelligence satellite series under various cover names. For a description, see: rob1blackops, 2017.
34 A historical example is the US Geosynchronous Space Situational Awareness Program satellite series. For a description, see: *Geosynchronous Space Situational Awareness Program*, 2020.
35 ESPI, 2020.
36 Aglietti et al., 2020.

been performed at the time when the Outer Space Treaty was codified (during the Gemini 6–7 flights in December 1965); therefore, it would have been possible to regulate them before they became commonplace.

3.3. Declaration and Enforcement of Security Zones Around Spacecraft

This section takes the cases described in the previous sections further by combining them. Considering the operational and security risks related to uncooperative rendezvous and proximity operations, a spacecraft operator can find it beneficial to declare a volume around their spacecraft to not only ensure safe and effective operations (as described in Section 3.1.) but also keep unwanted visitors away to prevent the harmful actions described in Section 3.2. The two unanswered questions related to this are whether such a declaration can be legal, and how such an exclusion can be enforced in the case of a breach into the security zone.

The declaration of a security zone can be similar to a declaration of an air defence identification zone (ADIZ). An ADIZ

> …serves as a buffer between international airspace and a country's territorial airspace…. Establishing such a zone allows a country to better monitor air traffic flying near its airspace and respond to aircraft that fly close to its airspace before the aircraft actually enter the airspace. Although such zones are not recognized as sovereign airspace by international law, it is customary for foreign aircraft entering such zones to identify themselves and seek prior authorization from the country controlling the zone before entering.[37]

However, an important difference between a space security zone and an ADIZ is that the ADIZ is a continuation of sovereign airspace, while a space security zone can only be the continuation of the internal physical volume of a spacecraft. During ADIZ operations, air defence forces of the country operating the ADIZ routinely fly out of sovereign airspace into international airspace to identify aircraft. Noncompliance with ADIZ rules[38] can only result in administrative actions before the noncompliant aircraft enters the sovereign airspace of the country (where the rules enforceable are not ADIZ-related but related to the military protection of sovereignty). At the same time, a declared space security zone, without the accompanying sovereign airspace where active measures are possible and legal, would be practically meaningless.

Still, we have seen and are seeing technological activities related to the enforcement of rules and active denial of navigation around spacecraft. The Soviet

37 Trent, 2020.

38 ADIZ rules typically require the filing of a flight plan, establishment of radio communications, use of automatic identification datalink systems and visual identification means, and compliance with the orders of the ADIZ administrator.

space station Salyut 3[39] carried the Rikhter R-23 23-mm compact aircraft cannon. The sole purpose of such a weapon on a spacecraft can be to provide the capability of firing upon another spacecraft. Considering the limited manoeuvrability of a space station, the only realistic use can be self-defence, that is, the destruction or disablement of an approaching spacecraft. Recently, France announced the plan of deploying small-size satellites equipped with lasers and kinetic weapons, as well as onboard weapons on the large satellites themselves to protect their military and national security missions' vital space infrastructure.[40]

According to the French announcement, these active protection measures could and would be used only when the hostile intent of the approaching spacecraft has been proven beyond doubt. However, this is questionable from a technical and practical point of view. The root of the French initiative was the approach and stationkeeping executed by the Russian Luch-Olymp electronic warfare satellite with the jointly operated French-Italian Athena-Fidus military telecommunication satellite.[41] The Luch-Olymp is equipped with radio receivers and is capable of intercepting signals directed towards its target satellite from the ground.[42] However, considering a typical uplink antenna beamwidth of 1.5 degrees and the distance between the communication satellite and uplink station of 40,000 km, the uplink station illuminates a circle with a diameter of roughly 1,000 km. Therefore, the Luch-Olymp only needs to approach its target within 500 km. Even with an extremely tight uplink antenna beamwidth of 0.3 degrees,[43] a 100-km approach is sufficient to intercept the signals. Stable stationkeeping at this distance is not a direct threat, but it is entirely sufficient to complete the mission.

Practically, these patrol systems could only be useful if they are used to prevent the approach into a predetermined volume around the spacecraft they protect; without that, the systems are purposeless in my opinion. With the spacecraft security zone declared, these patrol spacecraft can have the defensive depth to act. Therefore, the case falls back to the question of whether the declaration of a spacecraft security zone, within which the spacecraft operator (with the patrol spacecraft) can have the means to enforce restrictions on free navigation, is the declaration of a sovereign volume in space or not.

An analogy can be called for assistance – that is, the history of territorial waters, specifically, the cannon-shot rule. This is expressed as, '*Potestas terrae finitur, ubi finitur armorum vis*', which is translated as 'Power over the land ends wherever

39 On orbit between 25 June 1974 and 24 January 1975.

40 Lye, 2019.

41 Roberts, 2022.

42 Given the directional nature of the usual satellite uplink antennas, such signal interceptions are not possible (or at least not effective) when done from the surface or aircraft.

43 This is the -15 dB beamwidth of the GD Satcom 9.0m Cassegrain antenna at Ku band. The onboard receivers of a signals intelligence satellite are capable of compensating the signal loss compared to the -3 dB beamwidth commonly used in telecommunication link design calculations.

the force of arms ends'.[44] This practically means that state control over coastal waters extends as far out as the effective range of the coastal defence artillery. This somewhat vague definition was practically understood as 2–4 miles as measured from the shoreline.

The two situations can be easily compared. Both cases involve a physical location over which state control is undisputed. This is the land area of the state in the territorial waters' case and the internal physical volume of the spacecraft in the spacecraft security zone. From this location, a zone is extended outwards to the limit of the range of destructive capabilities the state can use, under its own sole discretion, to destroy or disable any craft that does not comply with the rules this state declares about navigation in the zone. Lasers or kinetic weapons carried by satellites are analogous to the coastal defence artillery protecting territorial waters. Their range, destructive capabilities, mode of employment, and employment itself are solely determined by the state that deploys the weapons. Based on this analogy, a unilaterally declared spacecraft security zone is in essence similar to the historical declaration of territorial waters; therefore, it is a declaration of sovereignty over a volume in outer space.

3.4. Section summary

This section examined the problems related to controlled access zones in outer space. From a practical point of view, the universal free access and freedom of navigation described in the Outer Space Treaty is not feasible. First, these are hardly possible with the current state of the technology. Second, and in my opinion more important, the age of trust between spacecraft operators (that existed during the early days of spaceflight) has come to an end. It is practically possible to approach any space object using another spacecraft. The real capabilities of the approaching spacecraft can stay hidden until they are actually employed, and this poses risks or even threats to the target spacecraft. The current legal regime does not provide rules or tools to mitigate these other than manoeuvring of the target (if it is capable of manoeuvring). This raises a question that is just as ethical as practical: Why should the target spacecraft subject itself to perceived coercion instead of having the right to stand its ground, deal with the threat, and continue to operate safely and securely?

There are regulated access zones operated or planned around space objects nowadays. However, these regulations apply to only those that are party to the agreements that established these zones and are not directly enforceable. Safe operation of these space objects depends solely on the good faith and voluntary professional behaviour of other operators.

The source of these risks and threats is the capability of approaching and stationkeeping with any space object by spacecraft with sufficient manoeuvring and

44 For the source of the quote and translation, see: Fellmeth and Horwitz, 2011, paras. 1–2.

navigation capabilities. This technology is not new, but its proliferation and automation makes this situation more severe.

We have often observed approaches to and co-orbital manoeuvring with uncooperating spacecraft. This technology can just as well be used for peaceful purposes as for hostile acts. The spacecraft systems necessary for one application group are just as usable for the other. For example, a space debris removal spacecraft needs very precise instruments to determine the movements and physical outline of the target debris, precise and agile manoeuvrability to approach, a grappling and manipulation toolset, and finally enough reserve orbital manoeuvring capability to physically remove the target debris to an appropriate disposal orbit. The very same onboard systems are necessary for a co-orbital anti-satellite system that is capable of observing as well as damaging or disposing of operational satellites during a conflict.

Therefore, it is understandable that operators of high-value satellites, which are considered critical national infrastructure or military mission vital infrastructure, plan to protect their spacecraft with real physical means. There are detailed arguments about how the UN Security Council or the belligerents could do this during conflicts.[45]

However, in the age of nonlinear and hybrid warfare,[46] the timeline and legal background for such a resolution or declaration are inappropriate. To start with, the UN Security Council can only adopt a draft resolution by affirmative vote of nine of the fifteen members and no veto from any of the five permanent members. Considering that three of the five permanent members (China, Russia and the US) currently possess spacecraft capable of noncooperative co-orbital operations for intelligence activities, along with the Security Council's ineffectiveness related to the Ukraine-Russia war (where one belligerent is a permanent member and is therefore capable of vetoing any draft resolution directed against its own interests), it is highly unlikely that such a resolution would be adopted during an actual conflict. Moreover, the very nature of hybrid operations is that the use of kinetic military means is just one part of the portfolio to be used by the aggressor. Most of the hybrid operations toolset is non-kinetic and below the threshold of conventional aggression.[47] This makes it very hard for the targeted operator or state to argue for a resolution.

It is argued that, to prevent a surprise attack and limit the effectiveness of intelligence gathering about the satellite, security zones should be created around spacecraft outside the time of conflict (or a different understanding is that the conflict is permanent and is actually ongoing even now). Such spacecraft security zones are meaningless without their enforcement, for which there is no existing international framework. However, individual enforcement of these zones is directly comparable to enforcement of the sovereign rule of territorial waters; that is, it practically equals

45 Stubbs, 2021.
46 Reichborn-Kjennerud and Cullen, 2016.
47 Treverton et al., 2018.

the declaration of sovereignty over a volume of outer space, which is contrary to the Outer Space Treaty.

It is desired that the international legal community, together with spacecraft manufacturers, operators, and space tracking service providers (both state and private organisations), develop a set of rules and regulations that are universally applicable to approach, rendezvous, and proximity operations. These rules must be tied to the existence and operation of the spacecraft itself and not to the operator or the state that registered it. This way, questions about sovereignty can be avoided. It must be noted, however, that enforcement of these rules remains unresolved.

Regulation of the rendezvous and proximity operations is not as hot a topic in international discussions as the question of destructive direct-ascent antisatellite weapons. However, in my opinion, considering the multiple-use nature of co-orbital operations and the possibility of below-the-threshold coercive applications, this regulation is even more important that the aforementioned debates and decisions about destructive antisatellite weapons.

4. Orbital Operations and the Status and Value of Space Objects

A spacecraft is valuable property. It can provide essential services and valuable scientific insights as well as be a key component in the defence and security framework of a nation. At the same time, defunct spacecraft or remnants of rocket bodies are considered drifting hulks and debris. However, on-orbit technologies (on-orbit servicing and manufacturing) can change this view. Launching masses of material into space is expensive, and the material already there is valuable.

On-orbit servicing missions can extend the life of orbiting spacecraft that lost some necessary capability to safely operate, such as their manoeuvring (stationkeeping) fuel,[48] power generation,[49] and attitude determination and control[50] capabilities. On-orbit servicing can reconstitute these capabilities. Modular spacecraft (typically, space stations and the Hubble Space Telescope) can also be repaired and

48 Various forces act on spacecraft, changing their orbits from their nominal mission orbits to unusable, even dangerous ones. Stationkeeping counteracts these perturbing forces to maintain a nominal mission orbit, and manoeuvring changes the orbit to adapt to new operational requirements. From the perspective of orbital dynamics, the two are similar. When the fuel usable for manoeuvring or stationkeeping is exhausted, the satellite cannot continue its services.

49 Most spacecraft use solar power as an on-orbit energy source. The semiconductor solar panels and chemical batteries get degraded during operation. When the power generation and storage capabilities fall below the level required by the spacecraft systems, the services need to be limited or ended.

50 To orient sensors or antennas, most satellites measure and control their orientation in space precisely. Without this capability, service provisioning for such satellites is not possible.

upgraded. With on-orbit maintenance, an inoperable satellite can be restored to being operational again with the investment of fewer resources compared to the launch of a new satellite. Finally, with in-space manufacturing complexes, it will be possible to recycle the material of space objects that are unfit for further use.

Differentiation between an operational spacecraft and a drifting hulk is not necessarily easy. Spacecraft can have many functions, and it is possible that these functions' operations do not cease at the same time. In extreme cases, even a spacecraft that completely lost its active functions can serve useful functions. One example is the Hungarian SMOG-1 picosatellite. This spacecraft carries an experimental material that interacts with the geomagnetic field to accelerate orbit degradation without requiring any power or control.[51] This experiment lasts for years, possibly up to a decade, during which all communications, control, computing, and power generation systems of the satellite are inoperational, but the satellite as a whole still executes one of its designed missions. Therefore, from a physical point of view, it is a drifting hulk no different from any other dysfunctional satellite or rocket body. However, from the operational point of view, it is a component of a technology experiment.

4.1. Operational and Inoperational Spacecraft

The Outer Space Treaty, the Convention on Registration of Objects Launched into Outer Space,[52] and the Convention on International Liability for Damage Caused by Space Objects[53] describe the rights and responsibilities of those who launch and operate space objects. They specify that the responsibility for safe and professional operation and for the damage caused by space objects is created by the launch (or launch attempt). According to Article VIII of the Outer Space Treaty, ownership of a space object is not affected even by its return to Earth, but it can be safely said that disintegration of a spacecraft in the atmosphere or during its collision with the surface means that the object ceases to be a space object.

The launching state is responsible for the damage caused by the space object. However, the practical application of this provision is not necessarily clear. During the early years of space activities, the number of space objects and their density in the volume of outer space made it highly unlikely that two uncontrolled space objects will collide before their orbits degrade into the atmosphere. As the advancement in technology trended towards more and more manoeuvrability and control, it could have been safely assumed that careful control of spacecraft would negate the risks of collision in the future.

As it turned out, the situation is entirely different. No fully reusable launch vehicles are yet developed, and therefore every space launch results in re-entries of

51 Alba Orbital, 2020.
52 UN General Assembly, 1975.
53 UN General Assembly, 1972.

stages that are not controlled, or the level of control is limited. A large part of the satellites launched nowadays (typically, smaller spacecraft) do not carry propulsion for orbit maintenance or collision avoidance.[54] These satellites are incapable of any action that could prevent a collision with another space object or property on the surface or in the airspace. Moreover, the onboard communication and identification systems (if there even is an identification system)[55] will usually reach the end of their lives much before the satellite reenters the atmosphere for final disposal. From here on, these satellites, of which hundreds are launched every year, are (according to the Outer Space Treaty and Liability Convention) still the responsibilities of their respective launching states, even though said states might have no means to track them (the capability of accurate space object tracking is not a legal prerequisite of a launch) and have absolutely no means to manoeuvre them. Moreover, as we have seen, such a space object can even be part of an active space utilisation project.

Therefore, according to the existing space legal regime, launch of a space object creates a responsibility that can last for decades, centuries, or even longer.[56] During a significant portion of this time, the launching state has no practical means to do anything to fulfil this responsibility and can only watch as the situation unfolds. The value lost in the case of a collision is highly dependent on the whether the satellite is operational, but right now, there are no objective guidelines to determine this, and the only source is the statement of the operator.

The only case up to now when a collision of an operational satellite with an inoperational one caused significant physical and monetary damage was the collision of Iridium 33 and Kosmos 2251.[57] Kosmos 2251 was a Strela-2M-class military telecommunications satellite. This type of satellite did not carry manoeuvring thrusters for orbit maintenance, collision avoidance, or (most importantly for our case) safe planned deorbit. The satellite ceased functioning in 1995 and was freely orbiting (on average) 800 km above the Earth surface, from where natural degradation can take many decades. Iridium 33 was a commercial telecommunications satellite operated by Iridium. Iridium satellites orbit at the same average altitude as the Kosmos 2251 did but carry manoeuvring thrusters, and the satellite was fully capable of executing the necessary orbit change to avoid the collision. However, the predictions available

54 Satellites of larger physical size and higher value typically carry manoeuvring thrusters for orbit maintenance and collision avoidance. In the case of a predicted collision between a satellite capable of an avoidance manoeuvre and another that is not, it is logical that the first does everything necessary to minimize the chance of any contact, even if it means the expenditure of its manoeuvring fuel (and therefore its lifetime).

55 The Orbital Whereabouts Locator (OWL) developed by C3S Ltd. is one example of an identification and tracking subsystem for small satellites. For technical and operational information about OWL, see C3S Electronics Development LLC, 2023.

56 The natural atmospheric drag removes the space objects within a few years from the lower volume of low Earth orbit. However, above the 1,000 km altitude, the drag becomes minimal, and the natural degradation takes at least decades. From medium Earth orbits and the geosynchronous altitude, natural forces can never remove the space objects.

57 Weeden, 2009.

to Iridium, based on public space tracking data, did not indicate a potential collision, only a close approach. The closest predicted approach was 117 m, which, while concerning, is not necessarily dangerous,[58] and subsequent predictions showed greater distances.[59]

Following the collision, many legal analyses have been published concerning the Liability Convention, which examine in detail the questions related to the event. As it turned out, even the applicability of the Liability Convention was questionable,[60] considering that Kosmos 2251 and Iridium 33 were both launched by the Soviet Union or its successor states (Iridium 33 was launched onboard a Russian Proton missile from Baikonur, Kazakhstan). My main concerns here are the questions of fault and duty.

To determine liability, first, the party who was at fault must be determined. Moving away from the actual case of the Iridium 33-Kosmos 2251 collision and generalising it as the collision of two generic satellites with similar capabilities, the determination of fault becomes very difficult.

Kosmos 2251 was completely passive, incapable of any collision avoidance or reporting of its position. However, it had ceased to execute its original functions 14 years before the collision and had no reason to be in space anymore. It was there because it was left there, knowingly abandoned by its operator. The only publicly available reliable source for its orbit was the public directory maintained by the US government; however, the accuracy of this information was known to be low. At the same time, it was known that the US government had more accurate orbit data but kept it highly classified. It can only be speculated that the Russian government had more accurate orbit data from its own space tracking systems.

The Iridium 33 was operating actively and was capable of manoeuvring; its radio emissions could have contributed to its tracking, in addition to the tracking data published by the US government. It had every reason to be present in space, and Iridium usually removed the satellites at the end of their useful lives by using the onboard thrusters (unless a satellite suffered a malfunction that rendered it uncontrollable). However, Iridium had no means to accurately predict that the collision was inevitable. Moreover, it was possible that a manoeuvre itself would create the geometry that led to a collision because of the uncertainties.

The question is, when does the chain of actions or inactions leading to the damage start? Is the launching state at fault because it knowingly launched a satellite that cannot be removed from orbit and might cause a collision decades or centuries later? Is the launching state at fault because it knowingly launched a satellite without accurate orbital surveillance capabilities to determine the relative path of other objects for the future planning of avoidance manoeuvres? While these technical challenges

58 Because of a lack of indirect effects such as a pressure wave, any approach that does not result in a direct contact is harmless.

59 Kelso, 2009.

60 von der Dunk, 2010. p. 201.

could actually be overcome, the ultimate challenge of final removal from orbit is often impossible to solve.[61] Considering the cislunar and interplanetary trajectories, the problem of abandoned spacecraft will be even more concerning because of the lack of space object tracking services.

4.2. Orbital Debris Removal

Since it is often impractical to install propulsion on a spacecraft to facilitate final removal from orbit, a business idea is growing nowadays to do the removal using specialised spacecraft.[62] These spacecraft need to be highly manoeuvrable and have adequate reserve fuel, sensors for precise approach and station keeping, and grappling manipulators to physically connect to the target satellite.

The timeline of an orbital debris removal mission can be envisioned as follows: The removal spacecraft is launched onto a suitable rendezvous trajectory (from either the ground or a storage orbit). It executes a rendezvous with the target and starts proximity operations to determine the actual status of the target and match relative movements and positions to set up the final approach geometry. Then, the removal spacecraft approaches the target and uses its grappling manipulator or other connecting device to attach itself to the target. The removal spacecraft then places itself and the attached target onto a transfer orbit towards the final disposal site. This final disposal can only occur by collision with a celestial body that removes all parts of the spacecraft from free orbital flight. Practically, in the Earth orbital region, an atmospheric reentry is a suitable final disposal. Reentry into other planetary atmospheres is also appropriate. A multi-mission-capable removal vehicle can detach from the target after the disposal manoeuvre to propel itself onto a storage orbit for its next mission.

In addition to this propulsive deorbit, other methods are being developed that do not require physical contact, such as directed energy effectors (laser brooms).[63]

Some space missions are already planned with this approach in mind. For example, satellite communications company OneWeb announced its partnership with

61 The energy required to remove a satellite from higher orbits is equal to the energy necessary to launch there from a lower orbit (where natural forces would remove them within a short timeframe). The following example uses a typical launch sequence used by Sea Launch during its operations (Sea Launch ceased its operations in 2014, after the conflict between Ukraine and Russia started, but it is used now because the equatorial launch did not require a plane change manoeuvre, and the energy requirement of the plane change is irrelevant now). The launch vehicle lifted the upper stage with a payload onto a roughly 200-km circular parking orbit. After the phasing coast, the upper stage changed the orbit into a Hohmann transfer trajectory (geostationary transfer orbit). Reaching the geostationary altitude, the upper stage or the payload itself circularised the orbit. The energy expended during the circularisation would be required again to put the end-of-life satellite onto a similar transfer orbit into the atmosphere. While this is technically not impossible, it is economically inviable.

62 *Top Space Debris Management Startups*, 2024.

63 Hedglin, 2018.

Astroscale to execute a removal mission and has incorporated grappling fixtures into the satellite design.[64] While OneWeb satellites can manoeuvre on their own and have designated reserve fuel for deorbit, this grappling fixture allows an independent-party spacecraft to safely handle the satellite in case of a failure.

Operators and service providers can handle liabilities and responsibilities in the contract they sign for the removal service. The situation becomes more complicated when an abandoned spacecraft needs to be removed. Of course, no spacecraft is truly abandoned, since the launching state always has liability and responsibility, but private operators can suspend their activities or go out of business, leaving uncontrollable drifting objects in orbit. In this case, it is unclear who has the right to act on the one hand and who is required to act to remove a space object on the other. When the technology becomes widely available, removal of the inactive space objects will be an effective way to keep space operations sustainable, especially in the low Earth orbit and geostationary orbit regions. In addition to the general cleanup of valuable orbital paths, emergency actions will be possible to prevent collisions.

There can (and will) be several events when time will be of the essence. A debris-generating collision in the higher regions of low Earth orbit, and especially in the geostationary orbit region, could pollute the region for centuries or longer. Cascading events (collision of debris pieces or collision of a debris piece with a third-party satellite) could prolong and increase the problem, and prevention of these cascading collisions in the most fragile regions is of utmost importance. The Liability Convention contains provisions about third-party damage; however, the main problem is pollution of the orbits. Space debris removal technologies will be able to prevent such collisions, even between unmanoeuvrable spacecraft, be they abandoned drifting hulks or operational satellites without propulsion. Numerous questions arise from this capability.

The first question comes from the uncertainty of the prediction of collisions. Only when two space objects come in physical contact can anyone be absolutely sure that the problem is real; however, any action is already late at this point. Up to the collision, the necessity of any action can be disputed. The operator of a spacecraft cannot be forced to enlist a space debris removal service to move their spacecraft, taking up the risks associated with such an action. Any external influence (an outside party, e.g. a state agency executing the manoeuvre) can be considered as a damaging action.

The second question comes from the future effects of the movement of the space object onto a different orbit. Up until the manoeuvre, it can be assumed that the spacecraft operator (ultimately, the launching state) is responsible for the consequences of the existence of the space object. However, the removal or collision avoidance manoeuvre introduces a variable most likely outside the control of the original operator. Again, when this removal or avoidance manoeuvre is done under a contract, the transfer of responsibility can be arranged between the parties. Nevertheless, when the manoeuvre is executed by an outside party to keep the orbits safe from a predicted potential collision, this transfer is uncertain.

64 Spacewatch.global, 2019.

4.3. Chain Event Effects and Indirect Consequences

With the number of space objects dramatically going up in the low Earth orbit region and the unsolved problem of final removal of abandoned satellites in the geostationary orbit region,[65] the probability of debris-generating collisions is increasing. While professional best practices, guidelines, and national regulations dictate the removal of space objects from outer space or at least from the most useful operational volumes, the timeframes within which this must occur is long, and the removal is not necessarily final. Even when the operator complies with the strictest guidelines, uncontrolled spacecraft pose significant dangers.

Satellites in low Earth orbit can be removed from space by lowering them into the atmosphere. Depending on the altitude of the operational orbit, this can happen without any propulsive manoeuvre, since atmospheric drag can exert enough force on the space object to complete the decay of the orbit within a set timeframe. This timeframe is set in international guidelines. For satellites orbiting higher, a propulsive manoeuvre is required to lower the orbit, so that natural forces can complete the removal. The time required for the orbit's decay depends on the manoeuvre.

Assume a satellite on a circular low Earth orbit at 1,000 km altitude. The time of its removal depends on the braking manoeuvre, when the originally circular orbit gets distorted to an elliptical orbit with periapsis[66] low enough for the atmospheric drag to have an effect. With enough fuel for the braking manoeuvre, the apoapsis can be lowered deep into the atmosphere or even to a negative altitude (collision course with the surface), so the ellipsis can be considered as a transfer orbit to destruction. This is the best possible manoeuvre, because the trajectory can be predicted accurately right to the descent into the dense atmosphere, and the manoeuvre can be timed to avoid any collision risk with space objects. However, this manoeuvre is energy-intensive (requires the most fuel), and the steep descent into the atmosphere can result in debris reaching the surface.[67]

65 The fate of the satellites in the geostationary orbit region is often misunderstood. It is true that the operators are obliged to remove the satellites at the end of their operational life from the geostationary altitude to a so-called "graveyard orbit." The exact altitude of this orbit depends on the physical properties of the satellite; however, it is generally 300 km above the geostationary altitude. The graveyard transfer manoeuvre removes the unmanoeuvrable satellite from the vicinity of the operational satellites, but this is not a final solution and does not remove the responsibility and liability of the spacecraft operator and the launching state.

66 Periapsis is a generic term for the point of an orbit closest to the central body. In the case of an Earth orbit, "perigeum," often abbreviated as perigee, is also used. The farthest point is called apoapsis, or in the case of an Earth orbit, the "apogeum" or apogee.

67 Most of the spacecraft structure is destroyed during aerobraking in the upper atmosphere. The steeper the reentry trajectory (the lower the perigeum), the shorter the time spent with aerobraking. While the peak temperature is higher during a steep reentry, the time available for the destruction of massive components is shorter. During a shallow re-entry (higher perigeum), more time is available for the destruction.

Less fuel expenditure results in an elliptical orbit where the periapsis is high enough so the satellite can survive the pass through periapsis and complete more orbits. Such a braking manoeuvre causes the satellite to slow down during the periapsis pass, and this slowdown lowers the apoapsis. The following periapsis pass will cause even more energy loss to lower the apoapsis again; ultimately, the orbit decays into the lower region of the low Earth orbit, and the satellite gets destroyed. During this elliptical orbiting, which can take years, the satellite periodically passes through the volumes most often used by productive satellites and crewed spacecraft. Every descent towards the periapsis and every ascent towards the apoapsis is a collision risk, and the orbit is constantly changing. During the time required for the decay, density of the upper atmosphere also changes (depending on solar activity), which further complicates the predictions. The advantage of a higher periapsis reentry is a shallower reentry angle, which means a more limited peak heating but a longer time spent in the upper atmosphere during the aerobraking, enabling a more complete destruction of the massive spacecraft structures.

Since the satellite slowly orbiting towards its destruction is not controllable or manoeuvrable, any collision avoidance manoeuvre must be completed by the other spacecraft. This means expending manoeuvring fuel otherwise budgeted for orbit maintenance, disruption of nominal operations, and potential loss of revenue as a consequence of both. While it can be argued that collision avoidance is a professional necessity during satellite operations, it is still a fact that disposals with unnecessarily long orbit decays place a burden on the operators of the spacecraft the satellite can collide with. A longer disposal manoeuvre (i.e. more orbits) raises the number of potential collision events with satellites in lower orbits. This time depends on the trajectory chosen by the operator of the satellite to be disposed of or by the disposal service provider.

A continuation of this case occurs when the elliptical orbits and periodical slowdowns themselves put the satellite to be disposed of onto a collision course with an unmanoeuvrable active (productive) satellite. In this case, the operator of the satellite to be disposed of complies with the regulatory requirement or professional duty to remove the inoperative spacecraft from orbit – but he also causes damage to another operator. Without the disposal manoeuvre, the collision would never have occurred. The collision would also not have occurred with a direct destructive reentry, but this would have put a financial burden on the operator of the inactive satellite that is not mandated by the current regulations.

These cases can be extended towards the general pollution of the outer space environment. With there being more and more abandoned unmanoeuvrable space objects and debris, some of them having predictable but practically “forever” orbits (medium Earth and geostationary/geosynchronous orbits), and some of them being on slowly decaying and constantly changing orbits, it can be argued that launching a satellite without collision avoidance capability is a mistake in itself. Moreover, any risk of a subsequent collision must be taken up by the launching party of the newer satellites, since they are launching into a known deteriorated environment. This

approach is ethically questionable, since it removes the burden from the shoulders of those who caused the deterioration of the space environment to start with. At the same time, this could be the basis of a completely new approach to space utilisation that would prevent even more problems in the farther future. This would also significantly slow down the current growth of the space economy, but with the emergence of propulsion systems for the smallest of satellites and the aforementioned space debris removal services, the technology is available for this approach. It should also be noted that with the proliferation of space situational awareness sensors and service providers, it could be possible to keep track of and account for the debris generated by subsequent collisions to enable the use of third-party damage provision in the space treaties; however, this might become impractical as the original launchers are further and further removed from being capable of doing anything to prevent future collisions.

There is also an emerging trend of space operations that can only be classified as reckless, but the Outer Space Treaty again does not contain provisions about this. A good example is a Chinese proposal to launch a satellite into the geostationary altitude, but with an inclination of 180 degrees, that is, right in the opposite direction of the orbits of every other satellite there.[68] Since the purpose of such a satellite would be space situational awareness data collection, it can safely be assumed that the satellite would carry advanced sensors that can provide enough warning for collision avoidance during the satellite's operational lifetime.[69] However, the usual problem arises again: After the end of the operational lifetime, when the sensors and propulsion systems are shut down, this retrograde orbiting spacecraft body would pose a collision hazard to others every 12 hours, and the relative velocity of a collision would be significantly higher than that of any collision anticipated in the geostationary altitude before.[70]

4.4. Section Summary

Outer space is an essential resource for our current and future life. It is vast, but still finite, and parts of it can be considered choke points that are very vulnerable. Every piece of mass launched to orbit is valuable one way or another, but this value is not constant during the time spent in space. The Outer Space Treaty and Liability Convention describe how spacecraft operators and launching states are responsible for safe space activities, but these are very challenging to apply in real life.

68 This orbit is often called "retro-geostationary," but this term is, while descriptive, technically incorrect.

69 He, Ma and Li, 2021.

70 Since objects in the geostationary/geosynchronous altitude all orbit with approximately the same velocity and the inclinations are also usually very close, the relative velocity during a collision would be much lower than what we see in the low Earth orbit space; therefore, the kinetic energy of the collision is also much lower.

There is no universally accepted and trusted space situational awareness service that could be used as evidence in legal disputes. The Iridium 33 collision showed that such services' usefulness is questionable even for practical operations because of the inaccuracies (and the data downgrade to protect the otherwise classified real capabilities).

In this environment, satellite operators are practically flying blind, both physically and legally. As we have seen, there are situations in which noncompliance poses less of a short-term risk than actual compliance with guidelines and regulations. Since the current legal regime allows very relaxed compliance, those who decide to act responsibly (and not just comply with the words of the regulations) lose their position in the race because of the cost of the systems required. Extra propulsion and fuel reserve to enable a direct destruction transfer orbit, subscription to a more precise space situational awareness service or development of own sensors, and similar technological addons are not required by law and are expensive. Moreover, in the most valuable orbital region, these guidelines and regulations do not even mandate the final removal of space objects, leading to what is called the "graveyard orbit," which practically involves just dumping cadavers onto the roadside.

To develop sustainable space operation frameworks, the burden of cleaning up the orbits and keeping them free from long-term clutter must be distributed among the users. This means creating regulations that prevent risky operations in the future and ensure the removal of existing risks. The main ethical problem is that the current risks were created during activities that were compliant with the regulations and guidelines existing at that time. Stricter regulations do not remove the objects currently present in space, which will remain there for a time much longer than what our society can handle currently.

This problem is comparable to the long-term storage of nuclear materials, but is more acute. We see several predictions of potential collisions every day, and the debris resulting from these collisions (if and when they occur) will not remove the risk but, on the contrary, increase it.

It is necessary for the international legal community to develop a completely new and universally binding set of regulations that control the access to and use of outer space, enabling equal access and, at the same time, providing for safe and sustainable use, ultimately leading to an operational structure that prevents the abandonment of space objects. This will make space activities significantly more expensive. These regulations will not handle all the risks (malfunctions will still occur) but will be a significant step forwards from the current position, where a sudden catastrophe can endanger a large portion of space assets that are not prepared to handle this. It is also necessary to develop a financial structure to support the removal of the already existing space objects that are considered beyond their useful life.

Satellites are critical national infrastructure and military mission vital infrastructure; therefore, sustainable space operations are also important for national

security. The current unsafe business practices endanger these space systems as well and can even pose an exploitable risk.[71]

5. Multiple-Use (Weaponisable) Space Systems

Just as it is very difficult to define where outer space is, it is also difficult to define what a space system can be used for. In addition to the usually understood "dual-use" – such as the use of space-based remote sensing or satellite communications to support commercial, government, and military operations from the same platform – new technologies enable more direct military applications. These technologies have peaceful or legitimate self-defence purposes but can be weaponised as destructive systems against spacecraft. The unregulated development of these technologies can create a race among space users to develop defensive technologies to counter them, and the testing and employment of the destructive systems will contribute to the degradation of the space environment described in Section 4.

A common property of these weaponisable systems is that they can be developed completely in the open, but their actual destructive properties can still stay hidden up to the moment of deployment against a spacecraft. This leads to destabilisation of the cooperative professional environment of outer space researchers, developers, and entrepreneurs. Moreover, they can lead to information and diplomatic operations against peaceful technology developers but can also be used as a perfect cover for weapons development.

5.1. Weaponisation of Orbital Debris Removal and On-Orbit Maintenance

On-orbit maintenance is a proven technology to extend the life of space hardware that otherwise would become an uncontrolled drifting hulk. It is beneficial from the economical point from view as well, because the production and launch of spacecraft that provides the orbital life extension is cheaper than that of a completely new productive satellite. Large telecommunications satellites typically reach their end of useful life because of the depletion of stationkeeping fuel or the degradation of power generation and storage systems. Currently, it is possible to provide stationkeeping to satellites that were built without any onboard system to enable this, as long as the orbital life extension spacecraft can grab a suitable structural part.[72] The

71 For a descriptive narration on this topic, see: the Chapter 1 of *Visions of Warfare 2036*, published by NATO Allied Command Transformation; Phillips and Cole, 2016, pp. 13–18.

72 Spacelogistics, 2021.

inclusion of specific attachment points, navigation aids,[73] and power connectors will make these operations easier and also enable the augmentation of the power system. Modular satellite architectures will enable even replacement of the payload, thereby further extending the useful life of the originally launched bus. Altogether, on-orbit maintenance will reduce the number of space launches necessary to provide essential space services as well as reduce the number of abandoned spacecraft, especially in the geostationary belt, which is in my opinion the most vulnerable orbital region.

It can be assumed that on-orbit maintenance will be performed as a cooperative action between the two spacecraft, and the target satellite will have at least limited attitude control. Even in this case, the approaching spacecraft need to have significant manoeuvrability. However, in the case of orbital debris removal, where the target space object is completely out of control, the approaching spacecraft needs even more agility and aggressive grappling tools. That is, because the target space object is out of control, the approaching spacecraft must be able to overcome its movements in all dimensions and degrees of freedom of movement to stabilise it and then move it to the disposal orbit.

It takes very little imagination to extend this scenario to when the target is a perfectly controlled productive satellite and the approaching spacecraft removes it against the will of the operator, attaches a device to it, or damages the satellite. All technologies required to do this (sensors, calculation of relative movements and interception geometry, orientation and translation manoeuvring, physical attachment, and manipulation tools) can be developed under the veil of developing a commercial or public service solution. At the same time, any commercial or public service solution development can be called offensive technology.

Co-orbital antisatellite operations, which this on-orbit maintenance or debris removal technology can enable, do not necessarily result in debris clouds and, therefore, are significantly more dangerous than the direct ascent antisatellite weapons (that always generate debris). Debris clouds resulting from kinetic collision of the direct ascent weapons have long-lasting effects on the space environment and can threaten the satellites of the aggressor. This can discourage the aggressor from using them. A co-orbital attack can achieve the same result without the release of debris, or with just a limited amount of it. However, note that when the goal of the aggressor is debris generation, co-orbital operations are capable of that also.

It must be noted that these systems have another vulnerability, which is independent of the intentions of their developers and operators. The cybersecurity of these on-orbit maintenance or debris removal spacecraft and their control systems must be extremely strong, considering their intended role. Without this, an adversary with access to the control systems can take over the spacecraft after launch and use it for their purposes, either preventing the intended mission or using it for an attack. These cyberattacks can be disguised as malfunctions, putting the blame

73 For information about navigational aids for proximity operations and grappling, see: Admatis, no date.

on the original operator. To flip this scenario, hostile deployment of a debris removal spacecraft can be presented as a consequence of a cyberattack by a third party. In this case, the hostile operator portrays itself as a victim, assuming the damage to their reputation but disguising their hostile intent.

5.2. Development of Direct Ascent Antisatellite Systems Under the Guise of Ballistic Missile Defence

Although direct ascent antisatellite weapons are not as flexible as co-orbital ones and their employment has far-reaching consequences, they still can have a place in the counterspace portfolio of a nation. They can support strong strategic messaging, and their information operation effect is also considerable.

Up to now, four dedicated kinetic kill antisatellite weapons[74] tests and one deliberate destruction have been executed:

- Shootdown of Solwind P78-1 by the US[75]
- Shootdown of FY-1C in 2007 by China[76]
- Operation Burnt Frost in 2008 (shootdown of USA-193 by the US), which was not announced as a test but as an emergency action to prevent remains of the satellite from reaching the surface after an uncontrolled reentry[77]
- Mission Shakti (shootdown of dedicated target satellite Microsat-R by India)[78]
- Shootdown of Kosmos 1408 in 2021 by Russia[79]

After the 2007 antisatellite weapons test by China and a similar test by Russia in 2021, the international community condemned such actions very strongly. The 2008 US action (Operation Burnt Frost) and the 2019 Indian test did not generate such strong reactions. One reason was that these collisions happened at a much lower altitude, and therefore much of the debris clouds re-entered within months; during the decay, the debris trajectories usually did not intersect with the orbits of productive satellites at higher altitudes.[80]

Of these tests and the USA-193 interception, only the ASM-135 missile used by the US in 1985 was a dedicated antisatellite weapon. The interceptor used by China in 2007 might also have been a dedicated antisatellite weapon that was later repurposed to a ballistic missile defence role, or vice versa. The SM-3 (US, 2008), Prithvi

74 Earlier antisatellite weapons carried nuclear warheads, and the test success criteria were that the warhead passed close enough to the target (so the target was present in the effective kill volume of the warhead). These tests did not generate debris. Kinetic kill weapons do not carry explosive or nuclear warheads, and they directly collide with the target and always generate debris.

75 Swopes, 2017.

76 Weeden, 2007.

77 Kelso, 2008.

78 Oltrogge, Kelso and Hall, no date.

79 Weeden, 2022.

80 A small percentage of debris got ejected onto higher orbits, but this was significantly less than the debris generated by the Chinese or Russian tests.

Mk II (India, 2019), and A-235 Nudol missiles all were originally ballistic missile defence weapons repurposed for an antisatellite role.

Ballistic missile defence is a very important capability for a nation to safeguard their citizens and allies, especially with the accelerated proliferation of intermediate-range ballistic missiles and hypersonic warhead delivery vehicles. It is an undisputable right of any nation to work on these defences. However, the capability requirements of midcourse interceptors and direct ascent kinetic antisatellite weapons are practically similar. The detection and targeting procedures are even simpler in the case of the antisatellite role (the time window is more relaxed in this case). Moreover, while the testing of direct ascent kinetic antisatellite weapons is practically universally condemned because of the resulting debris, testing of ballistic missile defence applications happens on suborbital trajectories, and the debris reenters immediately. The suborbital trajectory still enables the kinetic testing of targeting, interception, and manoeuvring. The general flight dynamics of the interceptor can be tested against simulated targets. This way, the antisatellite capability can be developed, tested, and validated without any actual debris-generating orbital interception.

Again, the dual usability of this technology opens the way to hide the development of systems that would destabilise and endanger the physical space environment and, at the same time, enable information operations and strategic messaging against legitimate defence-related development, thereby undermining cooperation in the professional community.

5.3. Multiple Usability of Electromagnetic Support and Defence Systems

The defence and national security use of Earth observation (usually called Intelligence, Surveillance and Reconnaissance [ISR]) is a very important supporting mission and can be a force multiplier in conflicts. Therefore counter-ISR is essential for ensuring operational security (OPSEC),[81] but at the same time, precise prediction of the overflight of adversary reconnaissance satellites[82] supports another information operation as well – military (or strategic) deception.[83]

To enable accurate overflight prediction (for concealment of real intentions or to show misleading information), the orbit of the overflying satellite needs to be known. The data for orbit determination can be obtained by active electromagnetic sensors, namely radars and laser ranging systems. These systems illuminate the satellite and measure the relative movement parameters by analysing the reflected signal. The orbit can be calculated from a series of measurements. Some satellites carry

81 OPSEC is the procedure for keeping essential elements of friendly information from the adversary, thereby keeping secret the intentions and activities of the force.

82 In NATO terminology, this is called satellite reconnaissance advance notification.

83 Military deception involves replacing the real essential elements of friendly information (kept secure by OPSEC) with fabricated ones and enabling the adversary to learn of these so as to shape the activities of the adversary into a desired direction.

retroreflectors to increase the reflected energy, but generally such measurements do not require cooperation of the target space object.

When it comes to the point in a conflict where active denial of information collection becomes a necessity, sensors on the overflying satellite can be influenced or overwhelmed by illumination with electromagnetic energy. Against radar satellites, this action is usually called jamming and is done by radio frequency emitters in the electromagnetic spectrum segment used by the radar.[84] Against optical satellites,[85] this action is called dazzling,[86] and it is done by laser emitters tuned to the wavelength(s) used by the camera of the satellite.[87] Jamming or dazzling does not damage the sensor, only obscures the image (or the reflected radar spectrum), making it unusable as a primary source of intelligence (at the same time, jamming or dazzling is an indirect indication of a high-value target).[88]

Although remote sensing of a sovereign state from outer space is generally considered legal, active denial of information collection in times of tensions, crises, or conflicts is also an understandable action. Since jammers and dazzlers do not cause permanent degradation of the spacecraft, it can be argued that the satellite is not damaged, even though a commercial operator can lose money by being unable to fulfil a contract.

However, the probability of permanent damage only depends on the energy absorbed by the sensor (or, in extreme cases, the satellite body). In this case, the illuminator becomes a directed energy weapon that can either take out the sensor (typically the optical sensor, but radar receivers can also suffer damage from high-power microwave irradiation) or damage other spacecraft systems. It must be noted that the damage threshold depends on the physical properties of the sensor, relative geometry of the sensor and illuminator, distance, and weather (transparency of the atmosphere); therefore, the damage can occur without the intention of the perpetrator. However, damage to other spacecraft systems is unlikely to occur this way, as these systems are more robust.

The problems with these electromagnetic energy systems are similar to those mentioned above. The outcome of the illumination depends solely on the energy output. All tracking and targeting systems are the same for different applications. Therefore, it is possible to fully develop and test the system under the veil of a space situation awareness sensor and complete the high-energy testing under laboratory

84 One example of satellite (and also airborne) radar sensor jammers is the Russian Krashuka 4. For more information, see: Army Recognition Group, 2024.

85 In military terminology, such optical payloads are usually called electro-optical, abbreviated as EO. On the one hand, this is unnecessary since no ISR satellite uses wet-film cameras nowadays; on the other hand, this can lead to misunderstandings since Earth observation is also abbreviated as EO. Therefore, the use of electro-optical is not recommended.

86 SPARTA, 2023.

87 One example of satellite optical sensor jammers is the Russian Peresvet. For more information, see: *"Peresvet" combat laser complex*, no date.

88 For a controlled demonstration of the effects of laser dazzling, see: Schleijpen, 2008.

conditions. Moreover, with the previously mentioned laser broom space debris removal technology, it is possible to do high-energy testing in the open. Everything written above about other multiple-use technologies concerning the destabilising effects and the potential information and diplomatic operations are true here also.

5.4. Section Summary

This section described several technologies that, on the one hand, can be very beneficial for safe and sustainable space operations but, on the other hand, are easily weaponised to be used for destructive offensive capabilities. A common point in these systems is that practically all the development and testing can be done under the guise of peaceful or at least defensive military technologies; meanwhile, the weaponisation is clearly understood by all concerned parties. This gives way to information operations and strategic messaging that distort and destabilise the otherwise useful development efforts and potentially undermine international cooperation.

Altogether, the proliferation of on-orbit maintenance, space debris removal, and space situational awareness sensor technologies (with their peaceful applications) would support sustainable space operations and could turn the tide of the currently deteriorating physical space environment. Meanwhile, ballistic missile defence interceptors, deployed in limited numbers, would discourage rogue states from offensive missile weapons development, while not breaking the existing equilibrium between larger nuclear powers.

It is desired that the international legal community develop safeguards, controls, regulations, and guidelines for the safe, secure, and transparent development of these technologies. It is necessary to prevent an arms race in counterspace capabilities, as well as prevent the degradation of the international political-diplomatic environment, which could be one outcome of uncontrolled development. These regulations need to be universal to prevent the reoccurrence of tensions that accompanied (for example) the termination of the Intermediate-Range Nuclear Forces Treaty.[89]

6. Summary

Outer space is a very dynamic environment. This statement is true for physics, business, and also the legal environment. International and national legislation is, on

89 The Intermediate-Range Nuclear Forces Treaty was a bilateral treaty between the US and Soviet Union/Russia to prevent an arms race in the field of nuclear weapons, against which the existing deterrent capabilities would have been inadequate. Unfortunately, the treaty did not follow the changes in the strategic environment, was used to undermine the preexisting understanding between the parties, and was ultimately terminated.

the surface, very active. However, fundamentals of the outer space legal regime are still based on the Outer Space Treaty and the related agreements and conventions, which were drafted in a very different era. The technology, politics, and economics of current space activities are far removed from those on which the Outer Space Treaty is based. The fact that the Five Treaties (Outer Space Treaty, Rescue Agreement, Liability Convention, Registration Convention and Moon Treaty) were successful in governing space activities for such a long time is not evidence of their versatility. It is just plain luck, which is supported by the diligence and professionalism of the actual space operators. Most of the provisions in the Five Treaties were never tested. No astronaut required rescue, only once did a state have to assume liability for any damage caused by a space launch, and a significant percentage of spacecraft were never registered. However, since nothing can be done about this, really nothing is actually done about it.

With the proliferation of space operations, increasing number of commercial space actors, and new technologies enabling new operational architectures and business opportunities, the time when the Five Treaties will be put to the test is nearing. It is my fear that they will fall short.

These treaties were signed during the Cold War, when the international relations related to space were much more cooperative than nowadays. Now, the space environment is described as "congested, contested, and competitive" or outright "disrupted, degraded, and denied." The multifaceted space environment is practically detached from the Five Treaties that should regulate it. We are at the end of the grace period during which this detachment still does not have practical consequences, but with the increasingly complicated space activities, a new set of regulations is necessary.

These new regulations need to address the shortcomings of the existing treaty system that are being exposed by the advancement of the technology and business. This chapter listed just a few examples of these shortcomings.

It is now absolutely necessary to, after roughly 80 years of space activities,[90] define where exactly is outer space. This definition will enable internationally recognised and binding regulations (comparable to those that exist now for airspace and the seas) for the physical domains concerned, namely the volumes above the airspace generally used for air operations. It will be necessary to define more than one volume to account for the physics of the upper atmosphere.

After the definition and delimitation of outer space, the question of zoning of outer space needs to be addressed. The current "free for innocent passage" approach is inadequate. It does not provide for operational safety, and especially not security. While the prohibition of claims of state sovereignty should be maintained, a regulated zoning around operational spacecraft is necessary. It is important for this protective zoning to be tied to the existence of the spacecraft itself, and not to the

90 The first vehicles reaching the volume usually considered as outer space were various test launches of the German V-2 (A-4) rockets, launched between 1942 and 1946 by Germany and the US.

owner, operator, or the party that files for the registration of the spacecraft. After this zoning, rules for the protection and defence of these zones can be defined.

No less important is the delimitation of operational spacecraft (that need to be protected) from objects that reach the end of their useful life (and that need to be removed safely to enable sustainable space operations for the generations to come). Just as the pollution of the space environment is a human action, this "cleanup" and maintenance need to be human actions also. Random forces of nature cannot be trusted with this job anymore.

Ultimately, the legitimate commercial and defence technology developments need to be delimited from weapons applications. War is part of our culture, and space is an effective supporter of the war efforts on the surface. Therefore, it is unavoidable that war will reach outer space. However, the current grey zone, in which warfighting technology is developed, is undermining the security of outer space even in peacetime; at the same time, it hinders peaceful and commercial research and development. Just as there are rules for military activities on Earth, such rules are (sadly, but unavoidably) necessary for outer space too. This task is made overly difficult by hybrid conflicts, where capabilities other than traditional military might are used.

Creation of these rules will require an international undertaking never seen before, involving states, international and supranational organisations, businesses, and academia. Since this program will most likely take decades, there is no reason for delaying the start any longer.

References

Admatis (no date) 'MSN (marker support navigation)' [Online]. Available at: https://admatis.com/msn-marker-support-navigation/ (Accessed: 12 October 2024).

Aglietti, G.S., Taylor, B., Fellowes, S., Ainley, S., Tye, D., Cox, C., Zarkesh, A., Mafficini, A., Vinkoff, N., Bashford, K., Salmon, T., Retat, I., Burgess, C., Hall, A., Chabot, T., Kanani, K., Pisseloup, A., Bernal, C., Chaumette, F., Pollini, A., Steyn, W.H. (2020) 'RemoveDEBRIS: An in-orbit demonstration of technologies for the removal of space debris', *The Aeronautical Journal*, 124(1271), pp. 1–23; https://doi.org/10.1017/aer.2019.136.

Alba Orbital (2020) 'Budapest University of Technology & Economics (BME) celebrates mission success of Hungary's first PocketQube satellites following Alba Cluster Two Launch', 23 October 2020. [Online]. Available at: http://www.albaorbital.com/new-blog/2020/10/23/budapest-university-of-technology-amp-economics-bme-celebrates-mission-success-of-hungarys-first-pocketqube-satellites-following-alba-cluster-two-launch (Accessed: 14 November 2023).

Army Recognition Group (2024) '1RL257 or Krasukha-4 jamming station', 18 July 2024. [Online]. Available at: https://armyrecognition.com/russia_russian_military_field_equipment/krasukha-4_1rl257_broadband_multifunctional_jamming_station_electronic_warfare_system_technical_data_sheet_pictures_video_10610156.html?utm_content=cmp-true (Accessed: 12 October 2024).

Bartóki-Gönczy, B., Sipos, A. (2022) 'A világűr és a légtér elhatárolása' [Delimiting outer space and airspace] in Bartóki-Gönczy, A., Sulyok, G. (eds.) *Világűrjog* [Space Law]. 1st edn. Budapest: Ludovika Kiadó, pp. 39–50.

Brockmann, K., Schiller, M. (2022) 'A matter of speed? Understanding hypersonic missile systems', *Stockholm International Peace Research institute*, 4 February 2022. [Online]. Available at: https://www.sipri.org/commentary/topical-backgrounder/2022/matter-speed-understanding-hypersonic-missile-systems (Accessed: 19 December 2023).

Bunn, M. (1984) 'Technology of Ballistic Missile Reentry Vehicles' in Tsipis, K., Janeway, P. (eds.) *Review of U.S. Military Research and Development 1984*. Pergamon-Brassey's International Defense Publishers, pp. 94–96. [Online]. Available at: https://scholar.harvard.edu/files/bunn_tech_of_ballastic_missle_reentry_vehicles.pdf (Accessed: 17 December 2023).

C3S Electronics Development LLC (2023) 'OWL: Essential Wearable for your Satellite', *C3S*, 2023. [Online]. Available at: https://c3s.hu/wp-content/uploads/2023/05/C3S_OWL_brochure.pdf (Accessed: 12 October 2024).

von der Dunk, F.G. (2010) 'Too-Close Encounters of the Third Party Kind: Will the Liability Convention Stand the Test of the Cosmos 2251-Iridium 33 Collision?', *Space, Cyber, and Telecommunications Law Program Faculty Publications*. [Online]. Available at: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1027&context=spacelaw (Accessed: 17 November 2023).

DuPont, A. (2005) 'ISS COTS Interface Requirements Document SSP 50808', *SlidePlayer*, 25 April. [Online]. Available at: https://slideplayer.com/slide/6541177/ (Accessed: 12 October 2024).

Durrani, H.A. (2017) 'The Bogotá Declaration: A Case Study on Sovereignty, Empire, and the Commons in Outer Space', *Columbia Journal of Transnational Law*. [Online]. Available at: https://www.academia.edu/35362196/The_Bogot%C3%A1_Declaration_A_Case_Study_on_Sovereignty_Empire_and_the_Commons_in_Outer_Space (Accessed: 10 December 2023).

EASA (2023) 'EASA Proposal for a Roadmap on Higher Airspace Operations', March 2023. [Online]. Available at: https://www.easa.europa.eu/en/downloads/137741/en (Accessed: 28 December 2023).
ESPI (2020) 'ESPI Executive Brief No. 38 In-Orbit Servicing: Challenges and Implications of an Emerging Capability' Vienna, 28 February 2020. [Online]. Available at: https://www.espi.or.at/briefs/in-orbit-servicing-challenges-and-implications-of-an-emerging-capability/ (Accessed: 29 December 2023).
Fellmeth, A.X., Horwitz M. (2011) 'Potestas terrae finitur, ubi finitur armorum vis' in Fellmeth, A.X., Horwitz M. (eds.) *Guide to Latin in International Law*. 1st edn. Oxford: Oxford Univrsity Press. [Online]. Available at: https://www.oxfordreference.com/display/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-1645 (Accessed: 12 October 2024).
He, By., Ma, Pb., Li, Hn. (2021) 'Properties of the lunar gravity assisted transfers from LEO to the retrograde-GEO', *Scientific Reports*, 2021/11, 18813; https://doi.org/10.1038/s41598-021-98231-1.
Hedglin, N. (2018) 'Policy Memorandum: The Case for Addressing the Crisis of Space Debris with Ground-Based Lasers', *Journal of Science Policy & Governance*, 12(1). [Online]. Available at: https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/hedglin_2018_jspg.pdf (Accessed: 17 November 2023).
ICAO (2006) 'Convention on International Civil Aviation Doc 7300/9 Ninth Edition', Chicago, 7 December 1944. [Online]. Available at: https://www.icao.int/publications/Documents/7300_cons.pdf (Accessed: 28 December 2023).
Kelso, T.S. (2008) 'USA 193 Post-Shootdown Analysis', *CelesTrak*, 27 February 2008. [Online]. Available at: http://celestrak.org/events/usa-193.php (Accessed: 27 November 2023).
Kelso, T.S. (2009) 'Analysis of the Iridium 33-Cosmos 2251 Collision', *Researchgate*, August 2009. [Online]. Available at: https://www.researchgate.net/publication/242543407_Analysis_of_the_Iridium_33Cosmos_2251_Collision (Accessed: 17 November 2023).
Laursen L. (2023) 'Civilian Satellites Descend Into Very Low Earth Orbit: Climate monitoring and telecom stand to benefit from 100 km orbits', *IEEE Spectrum*, 14 December 2023. [Online]. Available at: https://spectrum.ieee.org/vleo (Accessed: 19 December 2023).
Langbroek, M. (2022) 'Kosmos 482: questions around a failed Venera lander from 1972 still orbiting Earth (but not for long)', *The Space Review*, 16 May 2022. [Online]. Available at: https://www.thespacereview.com/article/4384/1 (Accessed: 12 December 2023).
Lye, H. (2019) 'French Defence Minister announces anti-satellite laser weapons', *Airforce Technology*, 26 July 2019. [Online]. Available at: https://www.airforce-technology.com/news/french-anti-satellite-laser-weapon/ (Accessed: 19 November 2023).
McDowell, J.C. (2018) 'The edge of space: Revisiting the Karman Line', *Acta Astronautica*, 2018/151, pp. 668–677; https://doi.org/10.1016/j.actaastro.2018.07.003.
Missilethreat (2021) 'Avangard', *Missile Threat*, 23 April 2021. [Online]. Available at: https://missilethreat.csis.org/missile/avangard/ (Accessed: 19 December 2023).
Oltrogge, D., Kelso, T.S., Hall, B. (no date) 'Indian ASAT Test Post-Event Analysis', *Center for Space Standards & Innovation*. [Online]. Available at: https://swfound.org/media/206441/india_asat_test_oltrogge_hall.pdf (Accessed: 27 November 2023).
Pelton, J.N. (2016) 'Urgent Security Concerns in the "Proto-zone"'. [Online]. Available at: https://www.mcgill.ca/iasl/files/iasl/3._j._pelton.pptx (Accessed: 28 December 2023).

Phillips, T.M., Cole, A. (eds.) (2016) *Visions of Warfare 2036*. Norfolk, VA: Allied Command Transformation. [Online]. Available at: https://www.act.nato.int/wp-content/uploads/2023/05/visions-of-warfare-2036.pdf (Accessed: 12 October 2024).

Pogies, Ch. (2021) 'The Cannon. A Tool for Delimiting Maritime Space', *Legal History Insights*, 14 June 2021. [Online]. Available at: https://legalhistoryinsights.com/the-cannon-a-tool-for-delimiting-maritime-space/ (Accessed: 17 December 2023).

Reichborn-Kjennerud, E., Cullen, P. (2016) 'Policy Brief [1/2016] What is Hybrid Warfare?', *Norwegian Institute of International Affairs*. [Online]. Available at: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf (Accessed: 23 November 2023).

rob1blackops (2017) 'History of the US High-Altitude SIGINT System', SatelliteObservation.net, 31 July 2017. [Online]. Available at: https://satelliteobservation.net/2017/07/31/history-of-the-us-high-altitude-sigint-system/ (Accessed: 12 October 2024).

Roberts, T.G. (2022) 'Unusual Behavior in GEO: Luch (Olymp-K)', *Aerospace Security*, 1 September 2022. [Online]. Available at: https://aerospace.csis.org/data/unusual-behavior-in-geo-olymp-k/ (Accessed: 19 November 2023).

Rocketlab (no date) 'HASTE'. [Online]. Available at: https://www.rocketlabusa.com/launch/haste/ (Accessed: 19 December 2023).

Sänger E., Bredt, I. (1944) 'A rocket drive for long range bombers', *Deutsche Luftfahrtforschung UM 3538*, August 1944. [Online]. Available at: http://www.astronautix.com/data/saenger.pdf (Accessed: 28 December 2023).

Schingler, J.K. (2020) 'Imagining safety zones: Implications and open questions', *The Space Review*, 8 June 2020. [Online]. Available at: https://www.thespacereview.com/article/3962/1 (Accessed: 27 December 2023).

Schleijpen, R. (2008) 'Laser dazzling of infrared focal plane array cameras', *Spie.*, 9 April 2008. [Online]. Available at: https://spie.org/news/1118-laser-dazzling-of-infrared-focal-plane-array-cameras#_=_ (Accessed: 12 October 2024).

Sipos, A. (2018) 'The Legal Status and Use of National Airspace', *Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae Sectio iuridica*; https://doi.org/10.56749/annales.elteajk.2018.lvii.11.141.

SKYbrary (no date) 'Scramjet'. [Online]. Available at: https://skybrary.aero/articles/scramjet (Accessed: 11 October 2024).

Spacelogistics (2021) 'MISSION EXTENSION VEHICLE (MEV): Award-Winning Satellite-Life-Extension Servicing Vehicle', *SpaceLogistics*. [Online]. Available at: https://cdn.prd.ngc.agencyq.site/-/media/wp-content/uploads/Mission-Extension-Vehicle-MEV-fact-sheet.pdf (Accessed: 27 November 2023).

Spacewatch.global (2019) 'UK's OneWeb To Use Altius Space Machines Tech For Space Debris Mitigation', *Space Watch*, 17 December 2019. [Online]. Available at: https://spacewatch.global/2019/12/uks-oneweb-to-use-altius-space-machines-tech-for-space-debris-mitigation/ (Accessed: 16 November 2023).

SPARTA (2023) 'Non-Kinetic Physical Attack: High-Powered Laser', *Space Attack Research & Tactic Analysis*, 22 April 2023. [Online]. Available at: https://sparta.aerospace.org/v1.3/technique/EX-0018/02/ (Accessed: 27 November 2023).

Stubbs, M. (2021) 'The Legality of Keep-Out, Operational, and Safety Zones in Outer Space' in Steer, C., Hersch, M. (eds.) *War and Peace in Outer Space*. 1st edn. New York: Oxford University Press, pp. 201–228; https://doi.org/10.1093/oso/9780197548684.003.0009.

Swopes, B.R. (2017) '13 September 1985', *This Day in Aviation*, 13 September 2024. [Online]. Available at: https://www.thisdayinaviation.com/tag/solwind-p78-1/ (Accessed: 27 November 2023).

Trent, M. (2020) 'Overview of Air Defense Identification Zones in East Asia', *Over the Line: The Implications of China's ADIZ Intrusions in Northeast Asia*, 1 January 2020, pp. 9–13. [Online]. Available at: https://www.jstor.org/stable/resrep26130.6 (Accessed: 29 December 2023).

Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K., McCue, M. (2018) 'Addressing Hybrid Threats', *Swedish Defence University*. [Online]. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf (Accessed: 23 November 2023).

UN General Assembly (1967) 'Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies', London, Moscow and Washington, 27 January 1967. [Online]. Available at: https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf (Accessed: 10 December 2023).

UN General Assembly (1970) 'Permanent Sovereignty Over Natural Resources of Developing Countries and Expansion of Domestic Sources of Accumulation for Economic Development', *United Nations Digital Library*, 11 December. [Online]. Available at: https://digitallibrary.un.org/record/201876/files/A_RES_2692%28XXV%29-EN.pdf?ln=en (Accessed: 11 October 2024).

UN General Assembly (1972) 'Convention on International Liability for Damage Caused by Space Objects' London, Moscow and Washington, 29 March 1972. [Online]. Available at: https://www.unoosa.org/pdf/gares/ARES_26_2777E.pdf (Accessed: 17 November 2023).

UN General Assembly (1974) 'Charter of Economic Rights and Duties of States', *United Nations Digital Library*, 12 December. [Online]. Available at: https://digitallibrary.un.org/record/190150/files/A_RES_3281%28XXIX%29-EN.pdf?ln=en (Accessed: 11 October 2024).

UN General Assembly (1975) 'Convention on Registration of Objects Launched into Outer Space', New York, 14 January 1975. [Online]. Available at: https://www.unoosa.org/pdf/gares/ARES_29_3235E.pdf (Accessed: 17 November 2023).

University of Wuppertal (no date) 'The mesosphere'. [Online]. Available at: https://www.iau.uni-wuppertal.de/en/home/atmosphere/mesosphere/ (Accessed: 11 October 2024).

Weeden, B. (2007) '2007 Chinese Anti-Satellite Test Fact Sheet', *Secure World Foundation*. [Online]. Available at: https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf (Accessed: 27 November 2023).

Weeden, B. (2009) '2009 Iridium-Cosmos Collision Fact Sheet', *Secure World Foundation* [Online]. Available at: https://swfound.org/media/6575/swf_iridium_cosmos_collision_fact_sheet_updated_2012.pdf (Accessed: 17 November 2023).

Weeden, B. (2022) 'Russian Direct Ascent Anti-Satellite Testing', *Secure World Foundation*. [Online]. Available at: https://swfound.org/media/207369/swf-russia-da-asat-testing-may-2022.pdf (Accessed: 27 November 2023).

Wilken, J., Callsen, S. (2023) 'Mission design for point-to-point passenger transport with reusable launch vehicles', *CEAS Space Journal*, 2023/16, pp. 319–322; https://doi.org/10.1007/s12567-023-00498-9.

Zak, A. (2011) 'Kosmos-482', *Russian Space Web*, 22 December 2011. [Online]. Available at: https://www.russianspaceweb.com/venera72_kosmos482.html (Accessed: 12 December 2023).

Zak, A. (2024) 'IS anti-satellite system', *Russian Space Web*, 5 March 2024. [Online]. Available at: https://www.russianspaceweb.com/is.html (Accessed 12 October 2024).

"Peresvet" combat laser complex (no date) *GlobalSecurity.org.* [Online]. Available at: https://www.globalsecurity.org/military/world/russia/vlk.htm (Accessed: 12 October 2024).

*Top Space Debris Management Startup*s (2024) *Tracxn*, 18 October 2024. [Online]. Available at: https://tracxn.com/d/trending-themes/startups-in-space-debris-management/__dL_W9uHJIB9gzbsnLjut_JIoZffwY3YWGa3ufa-BObI (Accessed: 16 January 2024).

Geosynchronous Space Situational Awareness Program (2020) *United States Space Force*. [Online]. Available at: https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197772/geosynchronous-space-situational-awareness-program/ (Accessed: 12 October 2024).

Chapter 11

Legal Aspects of Military and Defence Use of Outer Space

Katarzyna Malinowska

Abstract

This chapter examines the evolving landscape of military activities in outer space, considering the challenges it poses to existing space law. With an increasing number of nations utilising space for military and defence purposes, questions arise regarding the application of space law principles to these activities. This chapter delves into the notions of militarisation and weaponisation in outer space, exploring the role of space law in governing military applications and interpretation of the Space Treaties. The analysis extends to the evolution of international law, considering both binding and non-binding norms. Further, this chapter investigates the legal frameworks governing military use at the national and international levels, emphasising the need for regulations to address risks, including regarding space debris and sustainability concerns, as well as the prospective development of the European Union Space Law. Ultimately, the chapter aims to conceptualise the current and future integration of military aspects into the space regulatory framework and their interactions with contemporary challenges.

Keywords: space militarisation, weaponisation, space law, space wars, sustainability, EU Space Law, space defence strategy.

Katarzyna Malinowska (2024) 'Legal Aspects of Military and Defence Use of Outer Space'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 479–524. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_11

1. Introduction

Outer space has been the subject of interest for countries, especially their military sectors, since its dawn. This is because of its unique potential and capabilities related to the orbital and observation mechanisms.[1] Military use of space intensified during the Cold War, when the ASM-135 anti-satellite (ASAT) missile was developed and tested by the United States (US) Air Force in 1985. In 1980, other countries also started thinking about military use of space.[2] Moreover, space techniques showed their military potential for the first time in the First Gulf War during 1990–1991, when military forces relied heavily on remote sensing.[3] Moreover, although commercial use of outer space developed during the years and changed the optics from defence to civilian application of outer space, the military aspect has always remained, even if only behind the scenes. This aspect has recently returned to the main stage along with the increase in geopolitical tensions. The explicit symptoms of this shift can be seen in the ASAT tests conducted in recent years by China, Russia, the US, and India.[4] Nowadays, space applications have multiplied and are increasingly being used for military operations to serve reconnaissance, meteorology, communication, and navigation purposes, and they include space assets such as ballistic missile defence and ASAT weapons.[5]

The capabilities offered by the satellites have two aspects in relation to defence. First, they can help with Earth military operations, and second, they have increased in-space military capabilities, which some countries have recently shown in the form of ASAT tests. Experts have christened this trend as "space for defence" being transformed into "defence of space."[6] Regarding the first aspect – application of space techniques to military operations on Earth –remote sensing seems to be the most pertinent issue as it enables 'intelligence, surveillance and reconnaissance'.[7] This can also be called "space support for earth defence". Second, as regards military operations in space, this includes kinetic contacts between the space objects and proximity operations. Thus, it deals with defence and military actions in space. Both these aspects have a common denominator – protection of space-based assets.[8]

1 For example, the US Corona satellites and Soviet Russian Zenit satellites, launched in the 1950s, served military purposes. See also Polkowska, 2022.
2 Examples include Israel and South Africa. Ferreira-Snyman, 2015; Polkowska, 2022.
3 European Space Policy Institute (ESPI), 2020.
4 China in 2007, Russia in 2021, India in 2019, and the US in 2008.
5 According to data, as of 2018, the US military has over 170 satellites, Russia operates 97 military satellites, and China's military controls 100 satellites. Union of Concerned Scientists, 2019. See also Kehrer, 2019.
6 ESPI, 2020.
7 'A capability for gathering data and information on an object or in an area of interest (AOI) on a persistent, event-driven, or scheduled basis using imagery, signals and other collection methods'; ESPI, 2020.
8 ESPI, 2020.

Considering the above, several legal issues appear. Since the beginning of outer space exploration, two basic notions – militarisation and weaponisation – have been present, causing great concerns for both competing governments and lawyers. Thus, the question about the role of law, specifically space law, in governing the military application of outer space and its weaponisation seems to be one of the most pertinent in the era of space defence actions' intensification. The specific questions concern the application of space law to space military activities and meaning of the provisions included in the Space Treaties. This also concerns the application of the general principles of space exploration to defence and military actions in space, which are included in not only the Space Treaties but also various provisions of international law. In this context, the evolution of international law and its understanding must be investigated. When analysing the legal provisions, various types of rules should be considered with respect to their binding force and socio-political impact (hard law and soft law).

Thus, one most important research goal of this chapter involves checking what laws govern the military use of outer space and what principles guide their conduct. Related to the above, it is equally important to determine the borders of permitted actions in relation to the military use of outer space. The other aspect that must be considered is the institutional one, and it should be approached in two contexts: First, who is the law maker with respect to the military aspect of outer space, and which is the governing institution (i.e. what type of governance of the military aspect exists or should exist, at least on an international level)? The second legal issue concerns the national level, and the research objective within the above is how existing national laws should respond to the militarisation or weaponisation of space. Are the military (or defence-related) activities regulated by national space laws or should be (or are) exempted, and to what extent such exemption should work? Both contexts require ensuring safe and uninterrupted operations, so addressing the legal risks is necessary and involves analysing issues that belong solely to the space law and related domains (e.g. telecommunications law, export control measures, and cybersecurity regulations). Thus, the issues of space debris, the risk of losing control over the satellites, and the issue of sustainability in general must not be ignored. Nowadays, as the issue of sustainability of space activities has become pertinent, we cannot avoid analysing the military aspects of space activities in the context of sustainability. The ultimate objective of this chapter is to provide a concept of the current and prospective place of the military aspects of space activities within the space regulatory framework as well as their interaction with the currently significant issues (e.g. Zero-Debris Charter announced by the European Space Agency [ESA] in November 2023):[9]

9 ESA, 2023.

> The issue is of great importance and should also be addressed legally, for the reason that space war would have an immanent supranational character. The law may not be enough because of very many political aspects. Wars are always political in nature, so in a way they are always above the law, i.e. the law cannot completely prevent them, but it may be able to strengthen international control, which will have a preventive effect. And this is due to the fact that in the case of space, and its supranationality, the entire world community will always be interested, so the emphasis may be more on preventing excessive militarization and avoiding armed conflict in space.

To achieve the research goals specified above, first, the dogmatic method will be applied in the context of existing legal provisions, and a historic analysis will be conducted on the evolution of law and approach to the legal obligations related to space defence and military issues. An important and necessary method will be the comparative method, which will be applied for several purposes: comparison of different jurisdictions within space law and comparison between different branches of law. In addition, an empirical method will be used (to a limited extent) in the form of interviews with space sector experts.

2. Overview of the Existing International Space Regulatory Framework in the Context of Defence and Militarisation

This section will consider defence, militarisation, and weaponisation of outer space in view of the existing space regulatory framework, as well as other, related branches of law. Thus, the analysis will be conducted by reviewing the existing international laws, both space treaties, and space soft law. This will be followed by a discussion of the landscape of space-related international regulations. The second level of the regulatory framework that must be reviewed is the regional level, for which we chose the law of the European Union (EU), and the third one is the national level of space regulations. The analysis will be conducted based on the assumptions established in section 1. As a result, efficiency of the legal response to the needs of the defence policy in the field of outer space will be assessed.

First, it should be stressed that space law has always been related to the military aspects of outer space exploration[10] (as explained in section 1), and defence issues were the first impulses of states' interest in outer space endeavours. It was already so at the stage of the first satellites, such as Sputnik 1, which was launched in 1957 by the Soviet Union. Some authors indicated that 'it caused a crisis in

10 Kopal et al., 2011.

western military thinking and in consequence, a space race between USA and Soviet Union'.[11] The issue of a peaceful or military application of outer space endeavours was raised from the very beginning by not only lawyers but also policymakers,[12] and President Eisenhower suggested to extend the agreed rules with reference to Antarctica. Considering the period of the Space Treaties' negotiation, we can conclude that the military use of outer space was never questioned and has been subject to the observance of basic rules of international law.[13] Nevertheless, all state parties to the Space Treaties put on the table the founding principle of the peaceful use of outer space, which was repeated several times in not only the treaties but also resolutions of the United Nations General Assembly (UNGA) related to space exploration.[14] Thus, the clash between military needs and the emphasis on peace as the guiding principle of space exploration is one of the main paradoxes of international space legislation.

The result of the above paradox is the repeated question about the interpretation of "peaceful exploration" and "military purposes." In addition, academics around the world procured the whole list of pertinent legal aspects related to the military use of outer space. These include questions such as the following: What makes a space activity a military activity – the purpose of the mission or employment of military personnel and equipment? What is the frontier of passive (non-aggressive) use of outer space and its relation to peaceful outer space exploration? What are the legal consequences of using civilian systems for military purposes? What is a space weapon? What are the legal aspects of interference from Earth (unlawful interreference)?[15] The specific illustrative inquiries culminate in a broader interrogation concerning the role of law with respect to the military and defence issues in space. Linked to this overarching query is the inquiry into the most effective approach to regulate these facets while considering the prevailing geopolitical landscape. This examination encompasses diverse approaches to space law at the international, regional, and national levels of not only individual states but also the collective international community.

2.1. Assessment of the Current State of the International Space Regulatory Framework

To answer the questions to address the research objectives of this chapter, the main Space Treaties are analysed with the view of regulating the military issues in outer space. This refers to the following five main five treaties – (1) the Outer Space

11 Lyall and Larsen, 2018.
12 Ferreira-Snyman, 2015.
13 Cheng, 1997.
14 Ibid.
15 Lyall and Larsen, 2018.

Treaty,[16] (2) Liability Convention,[17] (3) Moon Agreement,[18] (4) Registration Convention,[19] and (5) Rescue Agreement[20] – which are jointly called the "Space Treaties".

First, the analysis requires identification of the military – oriented provisions of the Outer Space Treaty and recognition of their meaning. The Outer Space Treaty's preamble already emphasises the fundamental principle of space exploration – its peaceful use – which has implications for the interpretation of all its provisions, as well as the provisions of the other Space Treaties. On the other hand, a detailed analysis leads us primarily to Article IV, which is the main article directly regulating the military aspects of space exploration. Article IV sets the ban on weaponisation of space exploration.

According to Article IV Outer Space Treaty,

> States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.
>
> The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the Moon and other celestial bodies shall also not be prohibited.

Article IV Outer Space Treaty is often compared with the provisions of the Antarctic Treaty of 1959, which served as a politically agreed pattern for outer space, especially its Article 1, according to which,

> 1. Antarctica shall be used for peaceful purposes only. There shall be prohibited, inter alia, any measures of a military nature, such as the establishment of military bases and fortifications, the carrying out of military manoeuvres, and the testing of any type of weapons.
>
> 2. The present Treaty shall not prevent the use of military personnel or equipment for scientific research or for any other peaceful purpose.

16 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies,* 1967.

17 *Convention on International Liability for Damage Caused by Space Objects*, 1972.

18 *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, 1979.

19 *Convention on Registration of Objects Launched into Outer Space*, 1975.

20 *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*, 1968.

The content of Article IV is rooted in the provisions of the Partial Test Ban Treaty of 1963[21] and UNGA resolution 1884 (XVIII).[22] It also extends its scope to encompass orbits around the Earth, outer space, and celestial bodies, notably the Moon. Additionally, it mandates a selective demilitarisation of outer space. It draws inspiration from Article I of the Antarctic Treaty and is applicable to celestial bodies and the Moon. This segment advocates for comprehensive prohibition on the testing of all categories of weapons and a wide spectrum of military activities. Notably, it explicitly permits only the military activities that are delineated in its last sentence (use of the military personal and equipment), underscoring that any use must be 'exclusively for peaceful purposes'.

In the above context, it is most important to establish the meaning of "peaceful purposes." This point has been discussed by many scholars and in the forum of the United Nations; it has also been proposed by some space-faring countries.[23] The main controversy is whether the peaceful purpose equates to a non-military purpose. If so, the Outer Space Treaty would require the complete de-militarisation of outer space, which did not happen in practice even with several ratifications of the Outer Space Treaty. In fact, it seems that no country that is party to the Outer Space Treaty even seriously considered imposing such a restrictive interpretation and understanding of "peaceful purposes" while considering their strategic goals and intentions in using outer space. Thus, such an approach mirrored the proposed definition of militarisation, which assumes activities that do not engage satellites directly in the battlefield and are limited to reconnaissance and system supervision (see also the definition of militarisation proposed by Tronchetti as 'the use of space capabilities to support military operations occurring on earth').[24]

The above approach corresponds with the meaning of "peaceful purposes" as proposed by some states such as the US. It indicates that the notion of "peaceful" should be understood as non-aggressive rather than non-military or purely civilian. This interpretation has not been widely and explicitly accepted by both states and scholars;[25] nevertheless, nowadays, it seems to work as assumed based on the accepted state practice that military activities are permitted in space as long as they are non-aggressive (i.e. passive or defensive). To this day, interpretation of the term "peaceful" remains a source of contention, and such debates are poised to intensify

21 *Treaty Banning Nuclear Weapon Tests in The Atmosphere, in Outer Space and Under Water*, 1963. This treaty is sometimes also referred to as *the Limited Test Ban Treaty*.

22 UNGA, Question of general and complete disarmament, A/RES/1884 (XVIII) of 17 October 1963.

23 In 1958, UNGA formally endorsed Resolution 1348 (XIII), addressing the matter of peaceful utilisation of outer space. In response to this resolution, an ad hoc committee was convened to address the legal intricacies surrounding activities in outer space, as outlined in the paragraph. The committee's efforts culminated in a comprehensive report, which, among various recommendations, proposed the establishment of a permanent committee dedicated to overseeing legal aspects related to outer space activities; UNGA, Question of the peaceful use of outer space A/RES/13/1348 (XIII) of 13 December 1958.

24 Tronchetti, 2015.

25 Cheng, 1997.

the ongoing advancements in space techniques, technology, and their applications. Notably, application of the Outer Space Treaty to suborbital activities has become a focal point, influencing the permissible purposes of such endeavours. Specifically, the question arises about whether suborbital activities can align with international law while serving purposes other than those explicitly characterised as peaceful.

The other issue is the use of the military personnel and equipment, which is explicitly allowed by the Antarctic Treaty and Article IV Outer Space Treaty. Specifically, employment of military personnel or equipment for scientific research or any other peaceful purpose is expressly permitted. The main issue to be resolved in that respect is the legal consequence thereof for qualifying the activities undertaken as conducted for peaceful purposes. This signifies that the utilisation of military personnel does not inherently contradict peaceful objectives. This unmistakably allows for the establishment of military installations in space. In principle, if a state were to construct military bases, installations, or fortifications in outer space, such an undertaking would seemingly be deemed permissible under the Outer Space Treaty.[26]

Besides Article IV Outer Space Treaty, others articles may also help interpret the meaning thereof. In particular, Article III Outer Space Treaty should be considered, which seems to be a general guiding principle. According to Article III,

> States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.

This article clearly indicates that not only the Outer Space Treaty and other Space Treaties but also the general international law, such as the United Nations Charter[27] and others, will be applicable when analysing the militarisation and weaponisation of outer space. In that sense, these laws and treaties form the *Corpus Iuris Spatialis*. It should be remembered that the way the principles of the Outer Space Treaty are interpreted is related to the more general question about the position of space law within the realm of international law. The relationship between space law and the broader legal framework is subject to two prevailing perspectives. One viewpoint posits that space law operates as an autonomous and self-contained regime, distinct from the overarching international legal system. An alternative argument asserts that space law functions as a specialised branch, recognised as *lex specialis* within the realm of international law. The absence of a universally accepted definition of a self-contained regime complicates this discourse. However, one could conceptualise it as a framework of regulations with distinctive mechanisms for enforcement, specialised methods of interpretation and administration, and a standalone existence

26 Esparza, 2018.
27 *The Charter of the United Nations*, 1945.

that is not contingent on international law. In conclusion, the impact of Article III Outer Space Treaty designates space law as *lex specialis* when juxtaposed with the international law at large. However, it is imperative to recognise that such categorisation necessitates a case-specific evaluation. Furthermore, given the explicit reference to the United Nations Charter in Article III Outer Space Treaty, the subsequent subsection (sec. 2.2. of this chapter) delves into the intricacies of the relationship between the United Nations Charter and the field of space.[28]

The above touches on another significant matter – relevance of the Outer Space Treaty and other Space Treaties to other acts of international law. Especially important in this context is the United Nations Charter. According to Article 103 United Nations Charter, it shall prevail over the provisions of the Outer Space Treaty.[29] Such a statement has significant implications. Article 2 section 4 United Nations Charter is also critical in this respect. It forbids the use of threats or force against the territorial integrity or political independence of any state or in any other manner inconsistent with the purpose of the United Nations.[30] On the other hand, the United Nations Charter itself allows for self-defence actions. Namely, Article 51 of the charter provides for the right of self-defence of the countries:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

Thus, acting in self-defence shall be possible in outer space, but only within the limitations mentioned in Article 51 United Nations Charter. This means that self-defence should be exercised only to defend the personnel and space technologies. Moreover, self-defence must be proportionate and only in response to an attack and not be pre-emptive or anticipatory.[31] However, it is not fully clear how Article 51 United Nations Charter should be applied in relation to outer space, as it has not been designed for that purpose (and should only be applied to Earth); thus, there

28 See, for example, Hobe, 2019; ILC, A/CN.4/L.682.

29 Article 103 United Nations Charter: 'In the event of a conflict between the obligations of the Members of the United Nations under the present Charter and their obligations under any other international agreement, their obligations under the present Charter shall prevail'. See also Maogoto and Freeland, 2007.

30 Article 2(4) United Nations Charter: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations'. See also Tronchetti, 2014.

31 Lyall and Larsen, 2018.

are doubts about whether it is applicable at all. Therefore, we must not ignore that the relation between Article IV Outer Space Treaty and Article 51 United Nations Charter is not completely clear and seems to be of competing character. On the other hand, the 2008 draft Treaty on the Prevention of the Placement of Weapons in Outer Space[32] sustained the right of self-defence (which also appears in the 2014 draft as the individual and collective right of self-defence).[33]

One main issue (apart from the problematics of the peaceful purpose of space exploration) is the weaponisation of outer space. This issue raises concerns mainly with respect to the character of the assets placed in outer space, which are of a dual-use nature and can potentially be used for military purposes. This concerns all types of space applications – navigation, remote sensing, and telecommunications – which are not prohibited under space law. The distinction between military and non-military use of outer space is then quite blurred as regards the assets and not just their use purpose. This makes the interpretation of "peaceful purposes" even harder and in fact illusionary.

What is then the main difference between the militarisation and weaponisation of outer space? While militarisation has always been present, weaponisation – an advanced form of militarisation (defined as direct involvement of the satellites in war activities; Tronchetti[34] defined it as the deployment of weapons of offensive nature in space or on the ground with their intended target located in space) – has been recognised as unlawful and expressed as such in Article IV Outer Space Treaty.[35] The differences between militarisation and weaponisation concern both the type of spacecraft used and the purpose of using it. Thus, militarisation means the use of outer space by military spacecraft. In turn, weaponisation, although always perceived as a form of militarisation, goes a step forward and means placing in outer space devices designed to attack man-made targets in outer space. As regards the type of the spacecraft used, the dual-use nature of satellites must be mentioned. Note that all satellites are of such nature, even commercial ones, as they possess capabilities to provide services to the military, such as surveillance and guidance for munitions. Thus, the military character of outer space activities does not depend on the ownership of satellites but the type of services they render.

Given the abovementioned dual-purpose nature of many space objects, which blend military and civilian functionalities, coupled with the non-transparent disclosure practices of states concerning their space activities, evaluating the current level of weaponisation in space proves challenging. Nevertheless, comprehensive studies mapping the proliferation of various types of ASAT weapons have been published,[36] which affirmed that numerous states possess kinetic ASAT weapons de-

32 Mutschler, 2010, pp. 11–18.
33 For more details, see: Zahoor, 2017.
34 Tronchetti, 2015.
35 Polkowska, 2022.
36 Harrison et al., 2020; Peperkamp, 2020; Weeden and Samson, 2020.

signed for physically impacting a target. Notably, the US, Russia, China, and India have conducted tests involving such weapons on their own satellites, resulting in the generation of significant space debris that now orbits the Earth. Furthermore, a rise in non-kinetic "soft kill weapons" is evident, marked by cyberattacks targeting satellites, ground systems, and the communication links connecting them. Cost-effective disruptive techniques, including global positioning system jamming and data spoofing, pose an escalating military threat. While the trajectory toward progressive weaponisation of space appears discernible, determining whether this evolution can be characterised accurately as an actual arms race remains a complex task.[37]

To realise the practical consequences of this statement, first, the meaning of a space weapon should be tackled.[38] It is important to note that a space weapon has not been defined in international or local law. In consequence the meaning of "space weapon" is not coherently agreed upon, especially with respect to the question of whether ground-based weapons directed at objects in outer space (e.g. ASATs) also constitute space weapons or whether only devices located in outer space may be perceived as such. For example, the proposals of Tronchetti,[39] Duberti,[40] and Ferreira-Snyman[41] should be mentioned, which consider the broad and narrow meaning of a space weapon. According to the broad meaning, a space weapon is defined as a spacecraft and terrestrial-based system capable of destroying, damaging, or interfering with space assets. In turn, the narrow meaning points out that a space weapon should be limited to space assets whose specific goal is to destroy or damage an object in outer space; thus, the mere capability is not sufficient. If we focus on "capability," the broad meaning indicates that the space weapon is already there. Most space objects have such a potential (dual-use nature). Studies, such as by Mosteshar,[42] Tronchetti,[43] Khan,[44] and Blount,[45] propose a mixed definition.

In turn, the 2008 draft to ban weapons in space submitted by Russia and China proposed a definition of space weapons. According to this definition, a space weapon is any device placed in outer space, based on any physical principle, that has been produced specially or converted to destroy, damage, or disrupt the normal functioning of objects in outer space, on Earth, or in the Earth's atmosphere, or to eliminate a

37 Ibid.; Jakhu Jasani and McDowell, 2018.

38 On a practical basis, the new types of space weapons are of three types: Earth-to-space, space-to-space, and space-to-Earth. Moreover, systems can have both kinetic and non-kinetic effects that are either permanent or reversible. Earth-to-space weapons pose the greatest current danger and include direct-ascent ASAT weapons, which the US, China, India, and Russia have all tested, as well as directed-energy lasers and jammers. Center for Arms Control and Non-Proliferation, 2023; see also Preston et al., 2002, pp. 23–50; Zahoor, 2017.

39 Tronchetti, 2012.

40 Duberti, 2011.

41 Ferreira-Snyman, 2015.

42 Mosteshar, 2019.

43 Tronchetti, 2015.

44 Khan, 2017.

45 Blount, 2018.

population or components of the biosphere that are important to human existence or inflict damage on them.[46] Finally, the United Nations Institute for Disarmament Research proposed a definition wherein

> A space weapon is a device stationed in outer space (including the Moon and other celestial bodies) or in the earth environment designed to destroy, damage, or otherwise interfere with the normal functioning of an object or being in outer space, or a device stationed in outer space designed to destroy, damage, or otherwise interfere with the normal functioning of an object or being in the earth environment. Any other device with the inherent capacity to be used as defined earlier will be considered a space weapon.[47]

However, this definition was criticised as being too broad, as it includes all space objects.[48] Moreover, a weapon of mass destruction (WMD) refers to a nuclear, chemical, biological, radiological, or any other energy weapon (e.g. laser), and the Space Treaties include no ban on placing conventional weapons. In addition, there is no prohibition on testing, developing, or deploying (nuclear) Earth weapons systems for use in outer space or against space objects. Thus, ASAT tests are not explicitly forbidden by law.

The approach taken by the Outer Space Treaty with respect to the type of the weapon addressed in Article IV seems to reflect the technological landscape prevalent during the drafting and adoption of this treaty. Considering the technological advancements and emergence of conventional weapons' capabilities that were not envisaged during the negotiation of the Outer Space Treaty, there arises a pertinent question regarding the necessity of revisiting and amending the treaty. Notably, proposals for draft treaties aimed at prohibiting weapons in space, primarily championed by Russia and China in 2008 and 2014, were met with rejection, along with challenges in formulating a consensus on the definition of space weapons. Consequently, the current landscape relies on soft law instruments as the primary sources for guidance in the absence of a comprehensive legal framework.[49]

When considering the Outer Space Treaty provisions, Article IV is not the only one applicable. Not less important, although more indirectly, is Article IX, whose original purpose was related to avoiding potential harmful changes to the natural environment caused by space activities. Article IX visibly complements Article IV by establishing indirect limitations on military activities in outer space. It starts by stating that the exploration and use of outer space should be guided by the 'principle of cooperation and mutual assistance' and with 'due regard for the corresponding interests of all other States Parties'. The significance of Article IX in the context of

46 Ferreira-Snyman, 2015. Note that the 2014 draft included almost the same definition.
47 Cronin, 2009.
48 Cronin, 2009; Khan, 2017.
49 Tronchetti, 2012.

weaponry and military actions stems from its stipulation that if a state's activities, experiments, or nationals have the potential to cause harmful interference with another state's peaceful exploration and use of space, the initiating state is obligated to engage in consultations with the affected state before proceeding. Conversely, if a state anticipates that the activities or experiments of another state could lead to potentially harmful interference with its own peaceful exploration and use of space, it reserves the right to request a consultation with the concerned state.[50]

Another Space Treaty that should considered when discussing the regulation of military issues in outer space is the Liability Convention. Thus, the question of the applicability of the liability regime to military actions should be raised. The prevailing view is that the Liability Convention should not apply to actions regarding military outer space activities (or purposes), but it remains applicable if civil activities are involved. Other views also aim to exclude liability when self-defence actions are conducted. Such exclusions would only concern absolute liability. Moreover, no liability can be attributed to lawful attacks or military objectives, or to self-defence, necessity, or duress. However, absolute liability should be triggered if humanitarian laws are violated. Thus, it seems that liability in fault cannot be avoided.[51]

The Rescue Agreement seems neutral from the point of view of military actions in outer space. Such neutral wording was a result of intensive negotiations between the Soviet Union and US. While the Russian delegation sought to condition the duty to return astronauts on the launching state's compliance with the Declaration of Legal Principles, the US insisted on making it unconditional due to humanitarian reasons. According to the Soviet proposal, if the cognisant authorities of the state on whose territory an emergency landing is made were to believe that the astronaut is engaging in aggressive military activities or espionage, they would not be obliged to return the astronaut. Article 4 of the Declaration imposes an unconditional obligation to return the personnel of a spacecraft whose landing on the territory of a contracting party or outside the jurisdiction of any state is unintended or due to an accident, distress, or emergency.[52]

The final Space Treaty to be considered with respect to its application to military space activities is the Registration Convention. The subject matter of this convention relates strictly to the scope of application of the Outer Space Treaty and Liability Convention. Its purpose is to ensure the legal effect of their provisions in terms of the safety of outer space exploration and enforcing of the liability and responsibility regimes. Thus, it does not enlarge or clarify the scope of application but refers to the above treaties. The importance of the Registration Convention for the practical aspects of space activity is in introducing certain rules concerning the control, jurisdiction, and related registration requirements to be implemented by the launching

50 Esparza, 2018.
51 Kehrer, 2019.
52 Dembling and Arons, 1968.

states in their domestic laws.[53] Application of the Registration Convention is very general and includes all types of space objects, governmental and non-governmental. Although no exclusions have been provided with respect to the military or dual-use space objects, in practice, the states parties are reluctant to register and specify the military application of space objects. According to the clear provisions of the Registration Convention, all space objects, including their component parts as well as their launch vehicles and their parts, must be registered irrespective of their ownership, application, or purpose, whether it is scientific, technical, commercial, military, or humanitarian. Experts have pointed out that

> None of the Parties have described the objects as having military functions despite the fact that a large number of such objects do perform military functions as well. In some cases, the best they have done is to indicate that the space objects are for their defense establishments.[54]

An interesting evolution with respect to the scope of acceptable military activities can be observed from the time of negotiating the Outer Space Treaty in 1967 and the Moon Agreement in 1979. The main provision relevant to the issue in question is in Article 3 Moon Agreement, which says that the Moon shall be used by all states parties exclusively for peaceful purposes. Besides that,

> Any threat or use of force or any other hostile act or threat of hostile act on the Moon is prohibited. It is likewise prohibited to use the Moon in order to commit any such act or to engage in any such threat in relation to the Earth, the Moon, spacecraft, the personnel of spacecraft or manmade space objects.

In addition, Article 3 Moon Agreement repeats the provision of the Outer Space Treaty, saying that

> States Parties shall not place in orbit around or other trajectory to or around the Moon objects carrying nuclear weapons or any other kinds of weapons of mass destruction or place or use such weapons on or in the Moon.

and that

> The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on the Moon shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration and use of the Moon shall also not be prohibited.

53 Malinowska, 2017.
54 Jakhu, Jasani and McDowell, 2018.

It is important to note that the Moon Agreement concerns not only the Moon itself but also other bodies in the solar system (besides the Earth), including the orbits around and trajectories to or around it (Article 1 para. 2 Moon Agreement). Although the interpretation accepted by the United Nations Committee on the Peaceful Uses of Outer Space excludes from the above the Earth's orbit, it seems that the Moon Agreement also includes the void space. It is necessary to note that the Moon Agreement, adopted as the last of the five main Space Treaties, has been controversial since the beginning – not because of the military constraints but due to its restrictive approach to the extraction and utilisation of space resources. Finally, the Moon Agreement has been ratified only by 17 States and is not considered a binding treaty.

There are numerous other treaties besides the "big five" Space Treaties, among which three can be mentioned as applicable to space defence issues. Particularly, the 1963 Limited Test Ban Treaty prohibited the testing of nuclear weapons 'in the atmosphere; beyond its limits, including outer space; or under water, including territorial waters or high seas'. Furthermore, on 22 January 2021, the Treaty on the Prohibition of Nuclear Weapons[55] entered into force. Article 1 thereof stipulates that states shall under no circumstance '[d]evelop, test, produce, manufacture, otherwise acquire, possess or stockpile nuclear weapons or other nuclear explosive devices' or '[u]se or threaten to use' them. States that are party to the Treaty on the Prohibition of Nuclear Weapons are also prohibited from encouraging others to engage in any activity prohibited to a state party under the treaty. This prohibition of encouragement provides an additional layer that limits the use of nuclear weapons in space. Finally, the Convention on the Prohibition of Military or Any Hostile Use of Environmental Modification Techniques does not allow state parties to 'engage in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party'. This prohibition extends to outer space.

2.2. Space-Related Legal Regulations Applicable to Defence and Military Issues in Space

Considering that the general rules of international laws are to be applicable to the militarisation and weaponisation of outer space, as well as the general international laws, *ius in bello and ius ad bellum*[56] shall be applicable to outer space.[57] It is worth noting that general international law does not include any specific rules as regards war and military issues in outer space. On the other hand, as stated in the above section (2.1.), space law should not be treated as an isolated island but must be interpreted as an inherent part of the whole system of international law.

55 For the text of the treaty, see: United Nations Office for Disarmament Affairs, no date.
56 law of recourse to force (*jus ad bellum*) and law governing the conduct of hostilities (*ius in bello*).
57 Freeland and Gruttner, 2020.

2.2.1. Law of Armed Conflict and Space

The Law of Armed Conflict[58] and the Outer Space Treaty contain uniform concepts. Due to the nature of their use, it may appear that the Law of Armed Conflict dictates actions on land, and the Outer Space Treaty dictates actions in space. However, this could not be further from the truth. The proper way to examine an issue related to military action is by first examining the legal authority governing armed conflicts. The Law of Armed Conflict will always be the base point for an examination of whether a weapon or military action is permissible, because this law is designed to minimise suffering and prevent unnecessary destruction. The Outer Space Treaty is the law governing outer space, so it will be the first source of international law to consult in an analysis of permissible actions and objects in space. When these actions and objects are military in nature, the next source of international law necessary for such an analysis is the Law of Armed Conflict. This is because it builds upon the Outer Space Treaty articles. Before we can detail how the Law of Armed Conflict and the Outer Space Treaty work together, it is necessary to examine the key concepts of both.[59] Special attention should be given to the Geneva Conventions, which unequivocally mandate states to adhere to and ensure compliance with the conventions under all circumstances. Furthermore, the International Court of Justice, in an advisory opinion, authoritatively affirmed that the Law of Armed Conflict is applicable to 'all forms of warfare and to all kinds of weapons – those of the past, those of the present, and those of the future'. This determination suggests that the venue or nature of combat is immaterial, as the Law of Armed Conflict extends its application to any form of warfare and any weapon employed. Consequently, there appears to be no inherent limitation on the applicability of the Law of Armed Conflict to the domain of space.[60]

In instances where there is a significant threat to human life through an attack, applicability of the Law of Armed Conflict is indisputable. Nevertheless, ambiguity persists concerning whether the law is pertinent to situations in outer space involving technology, particularly satellites. The Law of Armed Conflict may eventually help fill some of the void left by the Outer Space Treaty, as explained in section 2 of this chapter. If conflict were to break out in space, the International Law of Armed Conflict or International Humanitarian Law would apply in so much as it places limitations on a state's activities in armed conflict wherever those hostilities take place.

58 The Law of Armed Conflict has not been a subject of detailed consideration under this chapter. However, it generally includes international regulations such as *the Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, 1949) *Geneva Convention Relative to the Treatment of Prisoners of War*, 1949; *Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, 1949; *Protocol Additional to the Geneva Conventions*, 1949; and *Protocol Relating to the Protection of Victims of International Armed Conflicts* (Protocol I), 1977.

59 von der Dunk, 2021.

60 Esparza, 2018.

Any application of humanitarian law would require a state to consider the specific physical characteristics of outer space to fully understand how a specific rule functions in the space domain.[61]

2.2.2. Export Control Regulations

The second area that is of a broader nature but has an enormous impact on space activities and its military character is the export control instruments. Export control forms a separate set of regulations concerning space activities, related to the fact that satellites and related equipment are always perceived as being of potential dual use. The best known regulation is the US International Traffic in Arms Regulations (ITAR),[62] which concerns launch vehicles and satellites. Although the rules have been relaxed in previous years, export controls remain fairly restrictive for free trade in the space industry,[63] as it involves not only manufacturing and exporting space projects but also launching and operating services and insurance,[64] as well as the export of goods, technology, data, and information. Other countries, especially those not within the EU, have adopted their own export control regulations; for example, Russia adopted measures similar to the US's ITAR. Russia's measures include a list of controlled items and technologies, along with the requirements to obtain approval. France,[65] Germany, and the United Kingdom (UK; Control Act 2002)[66] have also adopted independent measures.

Here, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement), founded in 1996, should also be mentioned.[67] This scheme does not regulate any particular regime of export control but is only a tool for international exchange of information on export controls by states that are parties to the Wassenaar Arrangement. It works

61 Blount, 2018.

62 It entered into force in 1999 as a result of enacting the Strom Thurmond National Defence Authorization Act for Fiscal Year 1999, the cause of which was the alleged commercial espionage by the Chinese. For more on the subject, see van Fenema, 2002. However, it should be noted that the ITAR it is not the only export control regulation in the US; the others are the Export Administration Regulations (concerning goods for dual use) and Office of Foreign Assets Control Regulations, focussing on countries and receivers; for more details, see: Creydt and Horl, 2011; Gerhard and Creydt, 2011; Zelnio, 2007.

63 The changes were introduced in 2001 by enacting the Satellite Trade and Security Act; changes were also introduced in 2013 by the National Defense Authorization Act, which allowed satellite technologies to be moved from the ITAR list to the Commerce Control List, which provides for less strict rules of export and allows the space operator to decide whether they are submitted to the regime or not and whether the Department of Commerce licence is required; see: Bank, 2011.

64 Creydt and Horl, 2011.

65 System of approvals issued by the Minister of Defence; see: Gerhard and Creydt, 2011.

66 In Germany, upon implementation of *the Foreign Trade and Payments Act*, a specialised central authority was established that was responsible for export. A similar concept has been adopted in the UK; Creydt and Horl, 2011.

67 Trautinger, 2016.

by establishing a list of controlled weapons and dual-use goods, and it imposes the obligation to report to the secretariat of the Wassenaar Arrangement (in Vienna) regarding export licences granted in a given state. The Wassenaar Arrangement is a multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies. It serves as a non-binding framework through which the 42 member states agree on which items should be controlled. The arrangement calls on states to disclose information regarding their export activities related to weapons and items appearing on the arrangement's two control lists – the List of Dual-Use Goods and Technologies and the Munitions List. Space technology is included in the agreed-upon control list, with an emphasis on launch vehicles, which can be repurposed as intercontinental ballistic missiles (ICBMs).[68]

Another international scheme is the Missile Technology Control Regime (MTCR), which was established in 1987. Its aim was to limit the spread of ballistic missiles and other unmanned delivery systems for biological, chemical, and nuclear attacks. It also utilises a list of controlled items and voluntary declaration of the states to limit the proliferation of such weapons. The MTCR is a set of international guidelines that seek to control the export of missile and rocket technology. It is a non-binding, informal political understanding among participating states that aims to limit the proliferation of such technology by controlling the export of goods and technologies that could contribute to delivery systems (other than crewed aircraft) for WMDs. The MTCR's technical annex on technology that should be controlled also includes space launch technology.

2.2.3. Spectrum Regulations

One of the most important areas of law related to space exploration and that undoubtedly affects military use is the international telecommunications law, which includes the Constitution and Convention of the International Telecommunication Union (ITU) and related regulations. Beginning with the preamble, peaceful use of telecommunications is emphasised, which corresponds with the fundamental principles expressed in the Space Treaties:

> While fully recognizing the sovereign right of each State to regulate its telecommunication and having regard to the growing importance of telecommunication for the preservation of peace and the economic and social development of all States, the States Parties to this Constitution, as the basic instrument of the International Telecommunication Union, and to the Convention of the International Telecommunication Union …, with the object of facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunication services….

68 Gerhard and Creydt, 2011.

Chapter VII of the ITU Constitution, titled 'Use of the Radio-Frequency Spectrum and of the Geostationary-Satellite and Other Satellite Orbits', discusses the meticulous regulation of outer space spectrum usage. Member states are mandated to minimise the frequencies and spectra employed to the extent required for satisfactory service provision. Recognising radio frequencies and associated orbits as limited natural resources, their utilisation must align with rational, efficient, and economical principles outlined in the Radio Regulations. This approach aims to ensure equitable access to orbits and frequencies for countries or groups, considering the unique requirements of developing nations and the geographic circumstances of specific countries.

What is essential for the peaceful use of spectrum is the prohibition of harmful interference to the radio services or communications of other member states, recognised operating agencies, or other duly authorised operating agencies that carry on a radio service, operate in accordance with the provisions of the Radio Regulations, and are obliged to take all practicable steps to prevent the operation of all types of electrical apparatus and installations from causing harmful interference to radio services or communications.

As regards military use of spectra, Article 48 ITU Constitution directly regulates the principles thereof:

> Member States retain their entire freedom with regard to military radio installations. Nevertheless, these installations must, so far as possible, observe statutory provisions relative to giving assistance in case of distress and to the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used, according to the nature of the service performed by such installations.

2.2.4. Bilateral and Multilateral Agreements

The inability to agree on a treaty basis has prompted the development of bilateral agreements, as exemplified by the US Space Command's data-exchange agreements with countries and organisations (including the ESA).[69] Thus, numerous bilateral agreements have been concluded, such as the New START Treaty between the US and Russian Federation, which entered into force on 5 February 2011, to establish limits on intercontinental-range nuclear weapons. In February 2021, both parties agreed to extend the treaty until 4 February 2026. This limits the location of non-deployed launchers for both mobile and non-deployed mobile ICBMs at certain facilities, including space launch facilities. Moreover, New START prohibits interference with the "national technical means," of which reconnaissance satellites are

69 National Aeronautics and Space Administration (NASA), 2023; Polkowska, 2022; SpaceWatch.Global, 2019.

an important component.[70] Such bilateral and even multilateral agreements, despite contributing to the peaceful exploration of outer space, do not have a positive impact on the international body of law, the rule of law in general, or the establishing principles or their interpretation.

2.3. Character of Legal Norms Regulating the Military Aspects of Outer Space Exploration

The analysis in the previous sections indicated that the provisions included in the Space Treaties do not always bring satisfactory results, especially in the context of imposing strict rules to sustain the peaceful use of the outer space and prohibit the weaponisation thereof. Therefore, a set of "soft law" measures have been adopted both at the United Nations' level and by other decision-makers or non-governmental authorities. The reasons for this are two-fold: (1) non-feasibility of adopting subsequent treaties and (2) necessity of interpreting the provisions for which a resolution seems an appropriate form.

Among the numerous instruments of non-binding nature, those adopted in the United Nations forum must be mentioned. The UNGA, through a series of resolutions, has endorsed five declarations and legal principles, along with the Space Debris Mitigation Guidelines. Of particular significance are the Guidelines for the Long-term Sustainability of Outer Space Activities, which, while not directly regulating defence or military matters, may exert considerable influence in these domains. It is imperative to ascertain their applicability to military activities and explore whether any reasons exist that exempt such activities from these regulations, should they acquire the force of customary law.

The other initiative that must not be ignored is Prevention of an Arms Race in Outer Space (PAROS), which dates back to the 1970s. A critical development emerging during the Tenth Special Session of the UNGA on Disarmament in 1978 resulted in the states acknowledging the necessity of adopting further measures and engaging in international negotiations to prevent an arms race in outer space. This aligned with the principles of the Outer Space Treaty. This also marked the formal inception of efforts related to PAROS.[71] In 1981, UNGA adopted its first two resolutions pertaining to PAROS, reflecting varied approaches to address space security concerns.

70 United Nations Institute for Disarmament Research, 2022.

71 According to Liu and Tronchetti, 2016,

> On 2 December 2014 the United Nations General Assembly (UNGA) adopted Resolution 69/32 entitled 'No first placement of weapons in space'. The adoption of Resolution 69/32, which has received little attention in academic circles, represents, instead, a development worth of consideration for at least three reasons: 1) It is the first time that the General Assembly passes a resolution addressing a specific Prevention of an Arms Race in Outer Space (PAROS) issue, namely the (prohibition of) placement of weapons in space; 2) it indicates that PAROS remains a central topic in the agenda of States; 3) its controversial adoption demonstrates that States maintain substantial differences on the approach to be followed to enhance the security of space objects.

UNGA Resolution 36/97 C on PAROS tasked the Committee on Disarmament with contemplating effective and verifiable agreements to prevent such a race and explore an agreement prohibiting ASAT systems. Notably, PAROS remained a draft, and the resolutions mentioned above constitute soft law measures. UNGA Resolution 36/99, dated 9 December 1981, focussed on the conclusion of a treaty on the prohibition of the stationing of weapons in outer space. This resolution urged the Committee on Disarmament to initiate negotiations for an international treaty aimed at preventing the arms race from extending into outer space.

The other soft law measure is the Hague Code of Conduct against Ballistic Missile Proliferation (HCoC).[72] This is a non-legally binding set of guidelines that regulate the area of ballistic missiles capable of carrying WMDs. As regards space technology, the HCoC seeks to prevent the use of space launch vehicle programmes to conceal the acquisition of ballistic missiles capable of delivering WMDs. To achieve this objective, the HCoC encourages member states to sign and ratify existing Space Treaties, particularly the Outer Space Treaty, Liability Convention, and Registration Convention. It also urges states to 'curb and prevent the proliferation' and to 'exercise maximum possible restraint in the development, testing and deployment' of ballistic missiles. The code further establishes a set of transparency and confidence-building mechanisms that would allow states to exchange information on ballistic missiles and space launch vehicle programmes, as well as the number of annual launches of such systems. It additionally proposes the exchange of pre-launch notifications that 'should include such information as the generic class of the Ballistic Missile or Space Launch Vehicle, the planned launch notification window, the launch area and the planned direction'.

The other type of soft law measures are formed as industrial or even particular countries' initiatives. The most recent example of such a bottom-up initiative is the Space Industry Statement in Support of International Commitments Not To Conduct Destructive Anti-Satellite Testing.[73] In that respect, the words of Kamala Harris regarding the ASAT ban seem symptomatic:

> Without clear norms we face unnecessary risk in space, … The United States will work with commercial industry and allies to lead in the development of new measures that contribute to the safety, stability, security, and long-term sustainability of space activities. Through this new commitment and other actions, the United States will demonstrate how space activities can be conducted in a responsible, peaceful, and sustainable manner. It's an attempt to lead by example, and demonstrate we're willing to make this commitment ourselves and then encourage others to follow.[74]

72 See more at: https://www.hcoc.at/.
73 See: World Secure Foundation, 2023.
74 Erwin, 2022.

Among such initiatives, the International Code of Conduct for Outer Space Activities (or the Code) proposed by the EU can be mentioned. It represents a first update in the approach to the regulation of conventional military activities in outer space, as well as in the interpretation of the PAROS issue. Although it is based on the Space Treaties, its rules seem more technical and practical. The Code stresses multiple times the importance of a peaceful and sustainable use of outer space as well as notes the importance of preventing an arms race in outer space. The entire Chapter II of the Code has been devoted to the safety, security, and sustainability of outer space activities. In particular, attention must be brought to the obligation/postulate to refrain from any action that brings about, directly or indirectly, damage or destruction of space objects unless such action is justified by (1) imperative safety considerations, particularly if human life or health is at risk; (2) the need to reduce the creation of space debris; or (3) the United Nations Charter, including to ensure the inherent right of individual or collective self-defence, which may also be applicable to military operations as a general principle. Moreover, the Code stresses the aspect of cooperation. The Code proposes a soft law instrument negotiated bilaterally to implement norms focussed on preventing behaviour that causes space debris. However, the Code failed because it depends too much on soft law to avoid providing key definitions and on the common interests of states in preventing the "tragedy of the commons".[75] Therefore, there was a call for a more a clear distinction between commercial and military activities and more balanced measures on the restriction of military activities in outer space.[76]

For the time being, ESA has initiated an ambitious concept called the Zero Debris Charter (or Charter hereafter),[77] which is to be acceded on a voluntary basis by organisations and institutions. As written in paragraph 3.2 of the Charter, 'any entity demonstrating a strong commitment to advancing space safety and sustainability' can sign the Charter and join the Zero Debris Community, 'without requiring the agreement of existing partners'. The Charter's guiding principles include the prohibition on internationally releasing space debris during space activities and the obligation to minimise unintentional generation of space debris.[78] Although the Charter's character is civilian, it may potentially impact military activities (e.g. ASAT tests).

The above analysis indicates that the dominant part of the most recent attempts to regulate space activities – which will also inevitably impact the military aspects of space activities – have a soft law character. However, the rapidly increasing number of such attempts has created a chance for establishing an international custom, which, according to Article 38 Statute of the International Court of Justice, can become a binding source of law. Thus, the bottom-up approach seems to have gained

75 European External Action Service, 2014.

76 Su and Lixin, 2014.

77 This was facilitated by ESA's Protection of Space Assets Accelerator and created and written by 40 space actors. The charter contains both high-level guiding principles and specific, jointly defined targets to get to Zero Debris by 2030.

78 Zero Debris Charter; see: ESA, no date.

popularity considering the pertinency of the legal issues and impossibility of the international community achieving a formal consensus. Therefore, this approach is proposed only by some states, international organisations, and influential non-governmental organisations.

In sum, it seems that hard law, particularly Space Treaties, do not work well as a means of regulating space security issues.[79] Therefore, the main burden falls on soft regulations. However, can we consider these regulations as law in the classical sense? Although the name contains an internal contradiction, "soft law" measures are in fact seeds of future law. They will take on such a dimension once the content of soft law instruments is placed in treaties or bilateral agreements or, with the passage of time, acquires the value of international custom and thus becomes a source of binding (hard) law.

3. EU Space Regulatory Defence Framework: Strategy and Law

This section is devoted to the EU's role in creating a common regulatory framework for defence and security in outer space.

3.1. EU's Space and Defence Strategy and Legal Instruments Applicable at the European Level

For the past few years, Europe has experienced a transformation in its approach to defence, specifically space defence. This involves a fundamental change within the EU, which, in addition to the member states, is itself becoming an independent stakeholder in this arena. Considering global trends, including primarily US actions, the EU in late 2008 began building its own space situational awareness (SSA) system, consisting of three separate segments: (1) space surveillance and tracking, (2) space weather, and (3) monitoring of near-Earth objects. The SSA system has dual purposes, with military components constructed based on military requirements set by the European Defence Agency (EDA). Moreover, rapid developments were observed in EU space programmes such as Galileo and Copernicus, which, while serving civilian purposes, also have obvious defence and security potential.[80] In the past two

79 Polkowska, 2022.

80 Kozioł, 2022. See: European GNSS Agency, 2020, para. 1, for the statement of Internal Market Commissioner Thierry Breton at the 12th Space Policy Conference in Brussels on 22 January:
Although it has been a taboo at the European level up to now, the time has come to break this taboo and to recognise that space is an enabler of security and defence, with a defence dimension for Galileo and a security element for Copernicus.
See also Messina, 2021.

years, this is further evident through adoption of the Common Security and Defence Policy, Permanent Structured Cooperation, European Defence Fund, etc., as well as creation of the Directorate-General for Defence Industry and Space.[81] Despite the integrated strategic action at the European level, the legal aspects of SSA remain ill-defined due to the EU's concerns regarding competence in this area.[82]

The Space and Defence Strategy (or Strategy hereafter) was announced in 2022 as part of the Strategic Compass, which called for a dedicated strategy to address the threats faced by European space assets. In parallel, the EU's security and defence activities, such as the European Defence Fund and Permanent Structured Cooperation, have increasingly integrated space in recent years. It should be stressed that evolution of the EU approach to space security and defence is in line with not only the EU's increased transversal relevance in the field of security and defence but also developments in the international environment (see section 4 for more details).

The EU Strategy is a steppingstone towards an action-oriented roadmap along three dimensions: (1) fostering the use of space systems and services for terrestrial security and defence activities; (2) addressing the security of European assets in space; and (3) aligning Europe's political, operational, diplomatic, and governance dimensions. Besides, the Strategy points to a difference between the "safety and sustainability" and "security and defence" aspects of space activities. When dealing with activities in space, the Strategy focusses on "security and defence", which addresses the protection of space assets against threats. Similarly, the Strategy considers the expansion of the security interest of the EU and its member states beyond the low Earth orbit, medium Earth orbit, and geostationary equatorial orbit (current location of the EU and national public and commercial assets) to reach cislunar space and the lunar surface.

The Strategy proposes actions to strengthen the resilience and protection of space systems and services in the EU. Several actions are proposed to achieve this objective, such as (1) proposing an EU Space Law to provide a common framework for security, safety, and sustainability in space that would ensure a consistent and EU-wide approach; (2) setting up an information sharing and analysis centre to raise awareness and facilitate exchange of best practices among commercial and relevant public entities on resilience measures for space capabilities; (3) launching preparatory work to ensure long-term EU autonomous access to space, particularly addressing the security and defence needs; and (4) enhancing the EU's technological sovereignty by reducing strategic dependencies and ensuring security of supply for space and defence, in close coordination with the EDA and ESA.[83]

81 ESPI, 2020.

82 Polkowska, 2022; Robinson, 2010. None of the EU member states enacted adequate legal provisions regulating this area, but at the same time, they are reluctant to adopt measures at the European level.

83 Directorate-General for Defence Industry and Space, 2023.

3.2. EU Space Law as a Denominator of the European Space Defence Strategy

As noted above, one action to implement the EU Space and Defence Strategy is promoting the idea of an EU Space Law. The concept of the EU space regulatory framework was first announced in late 2022 through a communication of the European Economic and Social Committee.[84] Soon after, it was presented as an inherent part of the Strategy (in March 2023), and the reasons were explained as follows:

> To enhance the level of security and resilience of space operations and services in the EU, as well as their safety and sustainability, the Commission will consider proposing an EU Space Law. It will encourage the development of resilience measures in the EU, foster information-exchange on incidents as well as cross-border coordination and cooperation.[85]

Thus, the main objective of the law is to complement the security information collected through monitoring of the EU space programme, Accordingly, an information exchange network could be established based on the EU Space Law and provide through the EU Agency for the Space Programme. Moreover, it was noted that EU Space Law would ensure a consistent EU-wide approach as well as joint communication for the EU Approach for Space Traffic Management. Moreover, the Strategy proposed that the EU Space Law would complement the implementation of the NIS 2 Directive[86] and the upcoming Cyber Resilience Act,[87] as well as other existing cybersecurity frameworks. Further, it will incentivise the uptake of cybersecurity requirements for critical digital products used in space. Thus, EU Space Law would set specific cybersecurity standards and procedures in the space domain.

All these goals seem indispensable for proper functioning of the space sector and ensuring a coherent approach in the EU territory; however, it cannot be ignored that the EU acts within the powers vested to it by member states of the Treaty on the Functioning of the EU**.** Thus, not only the content of the EU Space Law but also the competency to adopt such law should be considered. Therefore, the starting point is the EU's competence within the scope of space activities. The current framework

84 *Opinion of the European Economic and Social Committee on the Proposal for a Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2023–2027 (COM(2022) 57 final – 2022/0039 (COD)) and Joint Communication to the European Parliament and the Council: An EU Approach for Space Traffic Management – An EU contribution addressing a global challenge*; (JOIN(2022) 4 final), OJ C 486, 21.12.2022, p. 172–184.

85 Directorate-General for Defence Industry and Space (2023).

86 *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*. PE/32/2022/REV/2, OJ L 333, 27.12.2022.

87 *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*, COM (2022) 454 final.

is derived from the Treaty on the Functioning of the EU,[88] Article 189 of which empowers the EU

> … to promote scientific and technical progress, industrial competitiveness and the implementation of its policies". To this end the Union shall draw up a European space policy and promote joint initiatives, support research and technological development, coordinate the efforts needed for the exploration and exploitation of space" as well as to "establish the necessary measures, which may take the form of a European space programme, excluding any harmonisation of the laws and regulations of the Member States.

The EU is also authorised by the Treaty on the Functioning of the EU to establish any appropriate relations with ESA. As a result, the EU authority to act in relation to the national competences operates in parallel with that of the member states, meaning that member states retain their national authority to act within the space sector even if the EU undertakes actions in the same area (Article 4.3 Treaty on the Functioning of the EU). Given the current circumstances, the absence of harmonisation in European space laws is emerging as a hindrance to addressing the interests of European societies. With space recognised as a strategic domain, additional measures are imperative to fortify the EU's strategic posture and autonomy in space through regulatory interventions.[89] Consequently, ongoing analysis and consultations aim to delineate the necessary scope of European space law. Preliminary considerations underscore a pivotal focus on safety, security, and sustainability. Striking a balance between the civilian and commercial dimensions of space, while accommodating the defence aspects of space activities, is crucial without encroaching upon the internal laws of member states. It appears that the prospective EU Space Law will primarily concentrate on security aspects, diverging from commercial considerations already addressed by various member states in their laws on space activities. This shift is likely to influence the choice of legal instrument, with expectations leaning towards a regulation rather than a directive for the forthcoming EU Space Law.

4. National Level of Space Defence and Military Legal Issues

This section is devoted to the analysis of the chosen legal regimes of the most important space-faring countries with respect to space defence and military issues. In recent years, the space strategies embraced by major space powers, such as the US,

88 *The Treaty on the Functioning of the European Union* signed on 13 December 2007, 2012/C 326/01, OJ C 326, 26/10/2012 P. 0001–0390.

89 See: General Secretariat of the Council of the EU, 2024.

Russia, China, Japan, and India, share common objectives. These include the reorganisation of military space establishments; advancement of new capabilities for security and defence applications; and formulation of novel strategic postures, encompassing the extension of the operational domain to cislunar space. As this chapter focusses on regulatory issues, space and defence strategies of the given countries are explained solely as a background for the adoption of appropriate legal measures enabling the implementation of national strategies. The author chose to analyse the leading space-faring countries as well as countries that have engaged in activities in this field in recent years, such as the US, UK, China, and Russia. In addition, the Central and Eastern Europe (CEE) region is analysed together.

4.1. The US

The US pioneered the development of the doctrine on space control, officially acknowledging space as a "contested" domain in the late 1970s, particularly during the Strategic Defense Initiative of the 1980s. The US Air Force introduced the concept of "space control" in 1995. By 2001, the Rumsfeld Commission highlighted concerns about the potential for a "space Pearl Harbor", which could significantly compromise the effectiveness of the US Army. These perspectives quickly led to the consideration of ASAT weapons in space. The objective was to safeguard the advantages of space and prevent adversaries from accessing those same resources.[90]

The US announced its recent space defence strategy in June 2020. The announcement stated that 'the Defense Space Strategy is the next step to ensure space superiority and to secure the Nation's vital interests in space now and in the future'.[91] The Defense Space Strategy provides guidance to institutions, mainly the Department of Defense, to achieve the desired conditions in space over the next 10 years. The strategy's main objective is ensuring that 'the space domain is secure, stable, and accessible'.[92] The strategy includes a phased approach for the defence to move with purpose and speed across four lines of effort: (1) build a comprehensive military advantage in space; (2) integrate space into the national, joint, and combined operations; (3) shape the strategic environment; and (4) cooperate with allies, partners, industry, and other US Government departments and agencies.[93]

90 Pasco and Wohrer, 2023.

91 Department of Defense, 2020a.

92 Department of Defense, 2020b.

93 According to the Joint Chiefs of Staff, 2018, cited in Pasco and Wohrer, 2023, p. 6, the US doctrine provides for the possibility of deploying Offensive Space Control (OSC):
OSC operations consist of offensive operations conducted for space negation, where negation involves measures to deceive, disrupt, deny, degrade, or destroy space systems or services. Adversaries, both state and non-state actors, will exploit the availability of space-based capabilities to support their operations. In keeping with the principles of joint operations, this makes it incumbent on the United States to deny adversaries the ability to utilise space capabilities and services. OSC actions targeting an enemy's space-related capabilities and forces could employ reversible and/or non-reversible means.

Several US national regulations exist on the use of outer space, including the National Aeronautics and Space Administration (NASA) Act of 1958, Commercial Space Launch Act of 1984, and the most recent US Commercial Space Launch Competitiveness Act of 2015; these are supplemented by other regulations, including the Land Remote Sensing Act. The recent National Defense Authorization Act of 2020 implements the Defense Space Strategy and establishes the US Space Force within the US Air Force. This act identifies the new military service's mission set, composition, general duties, and chain of command. Moreover, in November 2023, the US revisited its laws on licensing space activities in the form of the Commercial Space Act.[94]

Analysis of these acts indicates that military aspects are regulated mainly from an institutional point of view. The National Defence Authorization Act provides for the establishment of the US Space Force as an armed force within the US Air Force and regulates its status, composition, and competencies. According to the respective rules, the Space Force shall be organised, trained, and equipped to provide for freedom of operations in, from, and to the space domain for the US; provide independent military options for joint and national leadership; and enable the lethality and effectiveness of the joint force.[95] Furthermore, the military/defence aspects are visible in commercial space law, where the powers of the Department of Defense prevail over the authority of the civilian administration if the security or defence aspects are involved in the mission.[96] This act expressly provides that the Department of Defense plays a vital and unique role in protecting national security assets in space, and the authority of the Secretary of Defense, as it relates to safeguarding the national security, cannot be overruled. In some matters, the competencies are shared with the Department of Transportation as regards SSA data, and information is shared with any entity consistent with the national security interests and public safety obligations of the US.

According to the newest Commercial Space Act adopted in November 2023, a part of the licensing process is the attestation regarding weaponisation of the mission, which consists of attestation by the applicant that the space object is not a nuclear weapon or WMD, will not carry a nuclear weapon or WMD, and will not be operated as a weapon or used for testing any weapon on a celestial body. However, these attestations concern only civil, non-governmental missions, as the essence of the act is to regulate non-governmental space activities. Thus, it seems that military activities are not subject to transparent regulations, such as preserving the sustainability of space. The act designates the Department of Commerce Office of Space Commerce as the sole authority responsible for the authorisation and supervision certification

94 House of Representatives, 2023.

95 The Space Force has both combat and combat-support functions to enable prompt and sustained offensive and defensive space operations and joint operations in all domains.

96 The Space Competitiveness Act also provides for some prevailing authorities for the Department of Defence.

process. It also grants the Office of Space Commerce the sole authority and responsibility for making determinations and placing conditions on certifications to ensure compliance with US's international obligations. The regulatory streamlining does not impact the existing Federal Communications Commission's authority in regulating spectrum and telecommunications satellites or the Federal Aviation Administration's authority in regulating launch and re-entry operations. For all forms of space activities, the military component excludes the application of regulatory measures, resulting in the presented acts.

4.2. France

France is among the most advanced and experienced countries in using space technology for military operations (e.g. the SPOT [short for Satellite pour Observation de la Terre] system). France has developed advanced satellites such as Helios and the Pleiades constellation, which conduct reconnaissance activities on behalf of the French military.[97] The French Space Defence Strategy was published in 2019 and is perceived as a key step in the evolution of France's military posture and, more broadly, of the current debate over collective security in space.[98] The French Space Defence Strategy serves primarily as a policy document articulating France's vision for the future of space defence. While conventionally addressing potential new threats and risks that could disrupt freedom of access and action in space, it goes beyond by outlining ambitions for capabilities to adapt to changes in the space environment and secure space support for the armed forces. Notably, the Space Defence Strategy introduces the possibility of actual military action in space and establishes a new doctrine, emphasising the need to define rules for engagement in space. Given its origin as a document commissioned by the French President, its purpose extends beyond presenting a purely military perspective; it aims to be a reference for expressing France's stance on space security within the international community.[99] The Space Defence Strategy only defines defensive operations in space, known in the US as "defensive space control." In this context, it mentions 'actions taken in space to protect our assets and discourage any aggression'.[100] While the US doctrine entertains the possibility of employing ASAT even in the absence of a specific threat in space, the French doctrine takes a more measured approach, emphasising the desire to ensure freedom in utilising the space environment under all circumstances rather than seeking complete control of space. The French Space Defence Strategy revolves around two primary operational objectives, the first of which involves the development of space surveillance for detecting and attributing responsibility for any hostile actions in various orbits using sovereign resources. This may be done in

97 Polkowska, 2022.
98 Pasco and Wohrer, 2023.
99 Ibid.
100 French Ministry for the Armed Forces, 2019.

collaboration with other countries, or it may be operated by allies or contracted to trusted operators. The Space Defence Strategy acknowledges the potential reliance on commercial resources in specific cases, contingent upon the nature of requirements; these cases relate to French military satellites, French commercial satellites, allied satellites, and EU satellites. The Space Defence Strategy implicitly aims to position France as a leading force in European space affairs and foster the creation of an allied military space community. The second objective is the defence of French interests in space.

The above strategy is developed based on the competency of the respective authorities licensing civilian space missions and is naturally not reflected in the French Space Law, which, though well-established, focusses on commercial application and does not set any requirements on governmental military space activities. Thus, according to Article 26 French Space Law,[101] the law does not apply to the launching and control of space objects, the needs of national defence, or the needs of vehicles whose trajectory passes through outer space, particularly ballistic missiles. Activities of the Ministry of Defence acting as the primary space-based data operator are not subject to the provisions of Title VII (which means that they are released from the obligations to report it to the public administration).

4.3. China

Since observing the space race between Moscow and Washington in the 1950s, China has actively pursued space capabilities as a symbol of national strength. By 1964, China had advanced its space programme significantly by sending an experimental biological rocket into space.[102] In 1970, the country achieved another milestone by launching its first satellite. Aligned with the emphasis on science and technological development integral to China's post-1978 economic reforms, the country accelerated the development of its independent space capabilities. During much of the initial decade of reform, the Chinese government prioritised the development or acquisition of satellites for practical applications, aiming to stimulate national economic development. As part of this strategy, numerous military aerospace projects were redirected towards commercial production.

The goals and principles of China's space activities were first laid out in a white paper titled 'China's National Defense in 2002'.[103] According to this document, China's intention was to implement a military strategy of active defence, and use of the space sector for this purpose was to involve various types of activities, including civilian, commercial, military, and security. According to the declarations, the Chinese

101 *Law* No. 2008-518 of 3 June 2008, regarding *Space* Operations (as amended by *Law* No. 2013-431 of 28 May 2013).

102 Goswami, 2018.

103 White Paper on China's National Defense, available at: https://china.usc.edu/white-paper-chinas-national-defense-2002.

government is opposed to arming space due to its existing nuclear purposes (as a nuclear deterrent) and the cost of such an arms race. However, in 2015, China recognised space as a military domain, and the defence white paper linked international security developments to the defence of China's interests in space. These assumptions were given final shape in 2016 in the National Security Law.[104]

China aspires to not only leadership but also dominance in the space domain. In October 2016, leadership of the State Administration of Science, Technology, and Industry for National Defense, under the Chinese Communist Party, suggested that China could achieve the status of a "space power" by 2030. Furthermore, it boldly asserted that by 2050, China would 'surpass and lead' in various aspects of space-related activities. This 2050 goal was reiterated by a spokesperson from the China National Space Administration in 2018.[105] In turn, as outlined in a State Council white paper released in January 2022, titled 'China's Space Program: A 2021 Perspective,' China's objectives for outer space are multifaceted. The white paper articulates that China aims to enhance its capabilities to better comprehend, freely access, efficiently utilise, and effectively manage space. Additionally, the goals include safeguarding national security, leading efforts in self-reliance and technological advancement, and fostering high-quality economic and social development. China also aspires to advocate for sound and efficient governance of outer space, contribute to human progress, positively impact China's socialist modernisation, and promote peace and progress for all of humanity.[106]

As regards Chinese space law, it should be noted that China currently remains the only space-faring country lacking a structured national space legislation by having enacted only two regulations dealing, respectively, with the launch and registration of space objects. This means that other important areas, such as remote sensing and telecommunications, remain outside the scope of dedicated legislation. The two adopted administrative measures concern the registration and licensing of civilian space missions.[107] These measures are expressly limited to civilian space endeavours. As stipulated in Article 1 of these measures, their formulation is driven by the objective of regulating the administration of civil space launch projects. This regulatory framework aims to foster wholesome development of the civil space industry, safeguard state security and public interests, and fulfil China's obligations as a state party to the Outer Space Treaty. Civilian space missions, as defined within the context of these measures, encompass the launch of spacecraft such as satellites

104 China is among a small group of countries developing counterspace technologies such as direct-ascent-ASATs, as well as non-destructive physical, electronic, and cyber technologies. For essential functions, key military space missions are increasingly relying on not a single satellite but multiple satellites to become more resilient to adversary attacks. Doucet, 2021; Polkowska, 2022.

105 Fravel, 2015.

106 China National Space Administration, 2022.

107 The 2001 Measures for the Administration of Registration of Objects Launched into Outer Space and the 2002 Interim Measures on the Administration of Licensing the Project of Launching Civil Space; see: Tronchetti and Liu, 2021.

within China's territory into outer space for non-military purposes. Additionally, the definition includes the launch of spacecraft, including satellites, by natural persons, legal entities, or other organisations of the People's Republic of China, with ownership either established or acquired through on-orbit delivery, into outer space from locations beyond the borders of China.

4.4. The UK

Since the inauguration of its first satellite, Ariel 1, in 1962, the UK has steadfastly pursued advancements in space exploration and aspires to secure a 10% share of the global space market by 2030.[108] In pursuit of this objective, the UK is resolute in upholding a regulatory framework that is not only competitive but also forward looking on an international level. Nevertheless, recent years have witnessed a heightened focus on space defence capabilities, as evidenced by the articulation of its defence space strategy.[109]

The UK issued its Defence Space Strategy in February 2022.[110] This strategy serves as a direct reinforcement of the integrated National Space Strategy. It outlines the vision for defence of the UK administration as a global participant in the space domain and elucidates how the Ministry of Defence intends to achieve its protect-and-defend goal through space-related capabilities, operations, and partnerships. The strategy aims to realise the ambition of becoming a significant actor in space. Its themes and principles are in harmony with and endorse the broader goals and key interventions of the national strategy, including the imperative to cultivate and expand talent. Furthermore, it aligns with all four objectives of the Integrated Review: strengthen security and defence domestically and internationally, build resilience, sustain strategic advantage through science and technology, and shape the future international order.[111] The most important thesis included in the UK's Defence Space Strategy is based on the defence investment through a blend of assured commercial and military grade solutions that will continue to increase flexibility, adaptability, tempo, resilience, and overall agility of the UK Armed Forces. Therefore, the intention is to maintain the UK's position as a leading military power and support UK's prosperity by enabling a safer, more secure, and sustainable operating environment, thus helping the UK space industry to continue flourishing. The principles underpinning the strategy include broadening and deepening multinational cooperation and improving cross-government collaboration.

At the regulatory level, the UK has made enormous progress by drafting and adopting modern space legislation. This started with the UK adopting the Outer Space Act 1986, which was subsequently amended by the Space Industry Act 2018 and

108 Rough et al., 2021.
109 Proelium Law, 2023.
110 UK Ministry of Defence, 2022.
111 Ibid.

supplemented by the Space Industry Regulations of 2021.[112] The legal framework apparently concerns civilian/industrial missions, and all military space matters belong to the competencies of the Ministry of Defence, whose Space Directorate cooperates closely with the UK Space Agency and is responsible for the Ministry of Defence's space policy and international coordination. The UK's military space programme is commanded and controlled by the UK Space Command, established in April 2021.

4.5. Russia

Russia considers outer space as a strategic region to enhance its military capabilities on Earth, provide intelligence and communication functions, and achieve international status and prestige as a space power. The dual utilisation of outer space aligns seamlessly with Russia's broader foreign and security strategy, characterised by a reactive stance towards US policy, while concurrently supporting the United Nations and favouring consensus-based multilateral negotiations.[113] The Russian military forces were reorganised in 2015 to create a separate space force. Russia increasingly integrates space services into its military, although it wants to avoid becoming overly dependent on space for its national defence missions because it views that as a potential vulnerability.[114] The nature of the Russian space ecosystem is rapidly evolving towards more profound and tightly integrated inclusion of the military programme. In this context, the Russian doctrine appears intricately woven to address the multifaceted challenges posed by modern warfare. The overarching conceptual framework involves the development of an integrated defence, with specific emphasis on aerospace defence forces. By integrating the Russian military infrastructure, the approach facilitates the treatment of an adversary threat as a comprehensive system. For the space military doctrine's implementation, Russia has cultivated an array of counter-technologies, thereby establishing the capacity to sustain a strategic position. The primary objective is to uphold the equilibrium of power within this domain. The Ministry of Defence is directing its attention towards three pivotal domains: deployment of direct ascent ASAT weapons, utilisation of disruptive systems targeting both space and ground infrastructures, and advancement of electronic and cyber-counter-space technologies.[115]

112 The Spaceflight Activities (Investigation of Spaceflight Accidents) Regulations 2021 establish a spaceflight accident investigation body and provide for the conduct of accident investigations; see The National Archives, 2021a. Moreover, the Space Industry (Appeals) Regulations 2021 outline the decisions made by the Civil Aviation Authority that may be appealed and set the procedures and timescales for making and deciding appeals; see: The National Archives, 2021b.

113 Eriksson and Privalov, 2021; Jackson, 2019.

114 Department of Defense, 2023.

115 Vidal and Privalov, 2023.

Russia adopted its space law in 1993 and took a specific approach as regards regulating the military issues.[116] The space law sets out the goals and principles of space activities, defines the licensing procedure, space activity financing, certification of conformity of space equipment, and touches on security and international cooperation in space. According to the law, the Federal Assembly has the power to determine the space policy of Russian Federation, the President has the power to implement space policy of Russian Federation and the Council of Ministers has the power to supervise space policy on space activities.

In 2020, the Russian Federation adopted a new set of licensing regulations through a federal decree. This was seen as a first step in preliminary work to improve legislation and remove administrative barriers in the development of the private sector. The role and functions of the space agency – Roscosmos – are defined in more detail in Federal Law No. 215-FZ 'On "Roscosmos" State Corporation for Space Activities', dated 13 July 2015.[117]

The specificity of the Russian space law concerns the explicit regulation of space activities conducted for the purpose of defence and security within the Russian Federation (Article 7). The tasks of overseeing these endeavours, collaborating with other ministries and departments, and together implementing long-term programmes and annual plans for the creation and utilisation of military and civilian space technologies have been entrusted to the Ministry of Defence. Specifically, the Ministry of Defence is authorised to develop draft programmes and plans, form and place state orders, use space technologies for defence and security purposes, engage in the exploitation of space technologies for scientific and economic purposes through contracts, and contribute to the maintenance and development of space infrastructure in coordination with the Russian space agency and other relevant entities. Additionally, the Ministry of Defence is responsible for providing normative technical documentation, participating in the certification of space technologies through contracts, ensuring the safety of space activities in collaboration with other state services, and undertaking other functions as determined by the Council of Ministers of the Government of the Russian Federation. Furthermore, the Ministry of Defence has the authority to mobilise any object of space infrastructure, including space technologies, as explicitly stipulated by the legislation of the Russian Federation. It also possesses the right to temporarily transfer idle objects under its jurisdiction to the Russian space agency through contractual agreements for utilisation in scientific and economic space activities.

116 Law of the Russian Federation on Space Activities, § 4, Art. 17 [Decree No. 5663-1 of the Russian House of Soviets].

117 Lukowski, 2023.

4.6. The CEE Region[118]

While all of the above space powers (except China) have developed both strategies and space laws, CEE countries still have a long way to go in this respect. They are in a specific situation: On the one hand, they have a space heritage gained from being behind the Iron Curtain; on the other hand, they still experience difficulties in catching up with Western Europe's value chains. This can also be seen with respect to the defence issues in space. These countries face many challenges: their geographical location is unfavourable to perform spaceflights, they face difficulties in gaining capital necessary to grow, and public clients have limited awareness of the space sector's benefits. Nevertheless, their location seems strategic from the defence point of view (as was proven since the beginning of the Russian aggression in Ukraine in 2022).

Differences between the regions of Europe are still apparent. Most Eastern European countries, due to their common history, have gained knowledge and experience from space activities during the existence of the Soviet Union and participation in Soviet space programmes.[119] However, over the years, each of these countries has developed different specifications in terms of management of space activities, expertise, funding mechanisms, priorities, and policy. As regards governance of the space sector in various CEE countries, the matter becomes even more complex. Organisation of the space sector differs significantly among CEE countries. In most cases, responsibility for the space policy remains distributed among many administrative bodies without clear indication of who is ultimately responsible for a certain area. This leads to inefficiency in the administration of the space sectors of most CEE countries. For example, in terms of cooperation with NASA, Poland was the only signatory of the Artemis Accords in the region for a long time. This changed after the Czech Republic (2023) and Romania (2022) signed the accords. Some countries in the region still do not have a specific institutional framework in the form of national space agencies, and space policy activities are the responsibility of certain offices within their ministries.[120] For example, in Slovakia, the responsibility for space is divided among the Ministry of Education, Science, Research and Sport; Ministry of Transport and Construction; Ministry of Environment; Ministry of Interior; Ministry of Economy; and Ministry of Foreign and European Affairs. In the Czech Republic, the Ministry of Transport is the coordinator of all space activities (through the Coordination Council for Space Activities). In Hungary, these duties fall under the Department for Space Policy and Space Activities of the Ministry of Foreign Affairs and Trade. Nevertheless, the recently adopted space strategies prioritise the

118 For the purpose of this Chapter, the CEE region is defined as including the following countries: Austria, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, and Slovenia, which are also recognised as signatories of the Three Seas Initiative.

119 For more details, see: Sagath, Adriaensenb and Giannopapa, 2018.

120 Klock and Aliberti, 2014.

establishment of a competent, central coordinating authority and creation of organisational and structural frameworks. As in the case of the Czech Republic National Space Plan 2020–2025, one goal is to improve the national institutional capabilities by establishing the national space agency as a single-access source for 'implementing a comprehensive package of measures to foster the entire domestic space sector.

Although majority of the CEE countries have adopted space strategies,[121] which also include the security and defence aspects, only Slovenia has adopted a national space law.[122] This state of affairs certainly delays the development of the space sector in these countries. Nevertheless, it provides an opportunity to address the challenges of the space sector, including the security aspects in the proposed legislation, such as the precise separation of competencies for civilian and military space missions, use of civilian missions for defence needs, and consistent regulation of sustainability requirements for each type of mission.

5. Governance of Outer Space in the Context of the Defence Policy and Law

The current legal framework at the international level, actions taken at the regional (EU) level, and the approach presented by individual states (defence strategy and space law) raise numerous doubts and concerns. Alarming events consisting of repeated ASAT tests are prompting the international community, especially legal scholars, to propose urgent measures to prevent the use of weapons in space. One example is the open letter issued on 2 September 2021 by the Outer Space Institute addressed to the United Nations; herein, the authors urged the UNGA to consider a treaty to ban kinetic ASAT tests.[123]

In sum, numerous weaknesses are revealed in the international space regulations that affect the security and stability of international behaviour in outer space due to the explicit gaps and vague meanings of the existing provisions. These weaknesses concern not only the regulatory framework in the strict sense but also the governance model. As mentioned several times in the chapter, at the global level, we can observe a matrix of various authorities vested in competencies in the field of space defence. These competencies seem to undergo serious transformations to comply with the changing paradigm of the space domain, as a part of the space force.

At the global level, the United Nations' role is constrained, leading to limited preservation of the foundational principles governing outer space exploration,

121 Poland adopted its space strategy in 2017, Hungary adopted its National Space Strategy in August 2021, and the Czech Republic approved its New National Space Plan in 2019 for years 2020–2025.
122 On 16 March 2022, the National Space Legislation was adopted by the National Assembly.
123 Byers et al., 2021.

particularly considering the diminishing connotation of the peaceful purposes of space endeavours. Given the prevailing geopolitical tensions, there is pervasive scepticism regarding the United Nations' efficacy as a policymaker and rule-setter. Consequently, coordination of defence and military matters on the international stage is more appropriately conducted through military and political alliances, such as the North Atlantic Treaty Organization.

Conversely, at the regional level within the EU, implementation of a space defence strategy entails a requisite reconfiguration of space governance. While the EU Agency for the Space Programme assumes responsibility for civilian programmes, recognising their dual-use capacity is imperative. Simultaneously, the EDA assumes a pivotal role in this context. The EDA's engagement spans a broader spectrum within the space domain, encompassing prioritisation and planning to support space capability development, engagement in research and technology activities related to space, and identification of common military requirements and defence user needs for space-based systems. This includes collaborative capability development and alignment with broader EU space policy objectives. The new Defence in Space Forum instituted under the auspices of the EDA plays a critical role in identifying military requirements, defining capability priorities, and fostering cooperation in space among EU member states.

As regards the responsibilities of national agencies, this sphere of the responsibilities of space agencies in defence domainis typically beyond their purview. In instances where defence and security issues arise in the context of civilian space missions, the authority of the military administration tends to prevail. Furthermore, military space operations typically fall under the exclusive control of the armed forces, often involving the establishment of specialised divisions for space command, as exemplified in the cases of the US and UK. However, it is crucial to emphasise that most of the investigated national space laws lack clarity regarding the delineation of administrative tasks and powers within this domain.

In France, implementation of the Space Defence Strategy initiated the first organisational changes, resulting in the establishment of the Space Command and the newly named Air and Space Force. Fuelled by the anticipation of potential military operations in space, this development signifies a significant stride towards a revised doctrine by 2030. The AsterX military exercises conducted in 2021, 2022, and particularly the latest one in 2023, which were held in conjunction with the large-scale ORION exercise in the south of France in spring 2023, underscore the Space Command's commitment to rapidly enhancing its operational capabilities. While the operations' message is primarily national, it also has European and international implications, aiming to cultivate national military space expertise through collaboration with foreign partners such as Germany, Italy, Belgium, and the US.

As mentioned above, institutional support is essential in the process of thinking holistically about military aspects in space. This mainly includes military issues, as well as those related to these issues, such as crisis management, which focusses on defence-of-space aspects (in connection with threats from ASAT tests, jamming,

cyberattacks, etc.). In this regard, experts call for the establishment of a management centre at least for the EU territory, which could lead to the coordination and sharing of space capabilities and intelligence information.[124] Europe, and the EU in particular, can model such coordination at the global level. Even if such an effect could not be achieved at the United Nations, an independent coordination centre could prove just as effective if may countries join it on a voluntary basis.

6. Summary and Conclusions

More and more countries are using or planning to use space for military and defence purposes, and the number of satellites used for military purposes is also clearly increasing. This means that maintaining the principle of peaceful use of space is becoming increasingly difficult. This also poses increased challenges to regulation and raises questions about the incorporation of military aspects into space law and the possibility of subjecting them to the principles of space law.

As seen from the analysis of individual states' strategies and space legislation, strategic documents are being developed specifically regarding the space defence domain at the international, regional, and national levels. This entails the institutionalisation of activities and separation of competencies between bodies responsible for space military issues and commercial space activities. While legal regulations are also being developed for the use of space, this is essentially taking place at the national level and only for civilian applications. Space law regulations that could apply to military matters remain in the regulatory grey area. They are not subject to licensing and are, consequently, also questionably subject to technical standards, if only for the prevention of space debris to ensure the sustainability of space exploration. Legal acts that are binding on states regardless of the purpose of the mission – that is, acts of international law – either contain very general regulations subject to inconsistent interpretations (e.g. Articles IV and IX Outer Space Treaty) or are non-binding (e.g. UNGA resolutions). As a result, the increasing scope of military applications is not matched by the development of a regulatory framework in this area, which undoubtedly poses a threat to the future of human activities in space, in terms of both security of space assets and security on the ground as an *ultima ratio*. In the face of this status quo, the solution may be bottom-up initiatives wherein states or regions (such as the EU) self-regulate and undertake initiatives that more states can join, such as the Zero Debris Charter. Conversely, for states still in the process of developing national regulations, their government military activities in space, while not inherently subject to licensing, should be subject to technical requirements, including space debris prevention and sustainability, on par with civilian missions.

124 Al-Akabi, 2015; Polkowska, 2022.

Among many regulatory grey zones, one most important on the international level involves determining what is allowed and prohibited under the Outer Space Treaty. Article IV is the main provision on which all scholars and diplomats focus while disregarding the whole body of the Outer Space Treaty and actions that may indirectly affect the fundamental principles of space exploration, even if not directly breaching Article IV. It is becoming increasingly clear that international space law (whether framed narrowly considering the treaties or more broadly) contains many gaps and instances of silence in its treatment of space military activities. These gaps may be filled with recourse to general principles until it becomes necessary and feasible to develop more explicit and concise international norms for emerging and novel space activities.[125] Besides the above, other fundamental legal issues appear in relation to the wording of Article IV. First, if the Outer Space Treaty regulates the purposes of exploring outer space, a question arises about whether we need the delimitation of outer space. Moreover, what approach should be taken for suborbital activities? Are they included in the assumptions of the Outer Space Treaty, or should they be subject to the air law? In addition, the issue of passage through airspace belonging to a state should not be ignored. According to Lachs, the above passage has become an international custom, but should it also be so when it is about a military action?[126] The conduct of reconnaissance from space aligns with the stipulations outlined in the Outer Space Treaty, but no discernible restrictions are evident.[127] International Space Treaties do not regulate SSA, and there is no obligation to disclose and share SSA data and information. Moreover, numerous national regulations in this area seem to establish restrictions in this regard. As a result, the only way forward is to regulate legal access to SSA data based on bilateral or multilateral agreements, and these, as is well known, depend on the political alliances of states.[128]

The current legal framework necessitates enhancement and continued development through the clarification of abstract principles, formulation of new legal norms, elimination of inconsistencies, and incorporation of the unique attributes of the space domain. Special attention must be paid to addressing cybersecurity in space and advancements in military technology. While the ideal scenario would involve the formulation of a new binding treaty, practical challenges, such as the states' difficulty in reaching a consensus, have impeded progress. Nevertheless, despite unsuccessful multilateral initiatives, an alternative avenue for development remains viable.

In a departure from the traditional treaty approach, it is not uncommon for independent expert groups to elucidate the application of existing international law,

125 Johnson, 2018.

126 Dissenting Opinions of Judge Lachs in *North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands)* Judgment, I.C.J. Reports 1969, p. 3; Ferreira-Snyman, 2015. Limitations arise when reconnaissance necessitates traversing a state's sovereign airspace; however, space-based reconnaissance appears to be permissible.

127 Willson, 2001.

128 Polkowska, 2022.

particularly humanitarian law, within a specific context. Noteworthy examples include the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2012). At present, two expert groups are actively working on manuals pertaining to warfare in the space domain – the *Woomera Manual on the International Law of Military Space Operations* led by the University of Adelaide and Exeter University and the *Manual on International Law Applicable to Military Activities in Space* by McGill University in Canada. While these manuals lack strict enforceability, their influence is acknowledged and relied upon by governments and armed forces; thus, they potentially guide space policy and military doctrines to prevent the hostile use of space weapons.

Despite uncertainties about the prospect of an arms race in outer space, the increasing risk of progressive weaponisation and space warfare demands attention. The rapid development of space technology has outpaced the evolution of existing space law, which is rooted in an idealised vision of space as a common heritage for peaceful purposes. This disparity between rules and practical realities introduces uncertainties about permissible conduct. Critical issues such as close-proximity operations, cyberattacks on space infrastructure, and ASAT tests lack adequate regulation within the existing framework. Moreover, the current legal framework is ill-equipped to provide definitive answers in the event of states engaging in space warfare. Strengthening the legal framework is pivotal to promote responsible use of outer space. Therefore, as argued, it is paramount to further develop and fortify the existing legal framework to ensure its adaptability to future challenges.

What is the roadmap for the regulation of military aspects in space? Who should take the initiative in this respect? While there is likely no one absolute answer to all these questions, considering the current framework and dynamics, it seems that the US and EU could eventually play a leading role as promoters of legal arrangements governing security issues, if only by promoting binding documents based on country adherence. Legal frameworks could be established in this realm through decisive, coordinated, and harmonised technical standards, as well as requirements for both governmental and private entities. Certification of activities, regardless of their military or civilian nature, appears to be a necessary course of action at all levels: international, regional, and national. They could eventually start as codes of good ethical practice for space operations and associated ground-based developments (e.g. initiatives of the Zero Debris Charter by ESA and the ASAT ban initiative by the US). There should be wide consultation with the public and interested stakeholders, including the civil society, in developing these codes. Addressing the issue of institutionalising such actions is also essential for this purpose.

References

Al-Akabi, C. (2015) 'European Access to Space: Factors of Autonomy', in Al-Ekabi, C. (ed.) *European Autonomy in Space: Studies in Space Policy*. Vol. 10. Cham: Springer, pp. 137–155; https://doi.org/10.1007/978-3-319-11110-0_9.

Bank, C. (2011) 'The Complexities of International Space Industry Contracts' in Smith, L.J., Baumann, I. (eds.) *Contracting for Space: Contract Practice in the European Space Sector*. London and New York: Routledge, pp. 133–150.

Blount, P.J. (2018) 'Dr. P.J. Blount' in Bragg, B. (ed.) *International Rules and Norms: Constraints on Space Operations: A Virtual Think Tank (ViTTa)® Report*. Boston: NSI Inc., pp. 8–11. [Online]. Available at: https://apps.dtic.mil/sti/pdfs/AD1095120.pdf (Accessed: 31 January 2024).

Byers, M. et al. (2021) 'Re: Kinetic ASAT Test Ban Treaty', *The Outer Space Institute*, 2 Septeber. [Online]. Available at: https://outerspaceinstitute.ca/osisite/wp-content/uploads/OSI_International_Open_Letter_ASATs_PUBLIC.pdf (Accessed: 31 January 2024).

Center for Arms Control and Non-Proliferation (2023) *Fact sheet: Space weapons*. [Online]. Available at: https://armscontrolcenter.org/fact-sheet-space-weapons/ (Accessed: 15 October 2024).

Cheng, B. (1997) *Studies in International Space Law*. Oxford: Oxford University Press; https://doi.org/10.1093/acprof:oso/9780198257301.001.0001.

China National Space Administration (2022) 'China's Space Program: A 2021 Perspective', *China National Space Administration*, 28 January. [Online]. Available at: http://www.cnsa.gov.cn/english/n6465645/n6465648/c6813088/content.html (Accessed: 15 October 2024).

Creydt, M., Horl, K.-U. (2011) 'Export Control Issues in Space Contracts' in Smith, L.J., Baumann, I. (eds.) *Contracting for Space: Contract Practice in the European Space Sector*. London and New York: Routledge, pp. 291–302.

Cronin, P.M. (2009) *Global Strategic Assessment 2009: America's Security Role in a Changing World*. Washington, DC: National Defense University Press.

Dembling, P.G., Arons, D.M. (1968) 'The Treaty on Rescue and Return of Astronauts and Space Objects', *Documents on Outer Space Law*, 1968/4, pp. 630–663. [Online]. Available at: https://digitalcommons.unl.edu/spacelawdocs/4 (Accessed: 31 January 2024).

Department of Defense (2020a) 'Defense Space Strategy', *Department of Defense Releases*, 17 June 2020. [Online]. Available at: https://media.defense.gov/2020/Jun/17/2002317654/-1/-1/1/RELEASE DEFENSE%20SPACE%20STRATEGY%20(FINAL).PDF (Accessed: 15 October 2024).

Department of Defense (2020b) 'Defense Space Strategy Summary', June 2020. [Online]. Available at: https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_defense_space_strategy_summary.pdf (Accessed: 15 October 2024).

Department of Defense (2023) 'Space Policy Review and Strategy on Protection of Satellites' *Department of Defense*, 12 September. [Online]. Available at: https://media.defense.gov/2023/Sep/14/2003301146/-1/-1/0/Comprehensive-Report-For-Release.Pdf (Accessed: 15 October 2024).

Directorate-General for Defence Industry and Space (2023) 'Joint Communication to the European Parliament and the Council European Union Space Strategy for Security and Defence' *European Commission*, 10 March. [Online]. Available at: https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en (Accessed: 15 October 2024).

Doucet, G. (2021) 'A Proposed Transparency Measure as a Step Towards Spaces Arms Control' in Steer, C., Hersh, M. (eds.) *War and Peace in Outer Space: Law, Policy and Ethics*. Oxford: Oxford University Press, pp. 247–264; https://doi.org/10.1093/oso/9780197548684.003.0011.

Duberti, (2011) 'The Legality of Space Weapons in International Law', *International Institute of Space Law*, 2011/1, pp. 80–87.

Eriksson, J., Privalov, R. (2021) 'Russian Space Policy and Identity: Visionary or Reactionary?', *Journal of International Relations and Development*, 2021/24, pp. 381–407; https://doi.org/10.1057/s41268-020-00195-8.

Erwin, S. (2022) 'U.S. Declares Ban on Anti-Satellite Missile Tests, Calls for Other Nations to Join', *SpaceNews*, 18 April. [Online]. Available at: https://spacenews.com/u-s-declares-ban-on-anti-satellite-missile-tests-calls-for-other-nations-to-join/ (Accessed: 31 January 2024).

Esparza, R.M. (2018) 'Event Horizon: Examining Military and Weaponization Issues in Space by Utilizing the Outer Space Treaty and the Law of Armed Conflict', *Journal of Air Law and Commerce*, 83(2), p. 333. [Online]. Available at: https://scholar.smu.edu/jalc/vol83/iss2/4 (Accessed: 31 January 2024).

European External Action Service (EEAS) (2014) 'DRAFT International Code of Conduct for Outer Space Activities', *EEAS*, 31 March. [Online]. Available at: https://www.eeas.europa.eu/sites/default/files/space_code_conduct_draft_vers_31-march-2014_en.pdf (Accessed: 31 January 2024).

European GNSS Agency (2020) 'Space is an Enabler of Security and Defence', *European Union Agency for the Space Programme*, 7 February. [Online]. Available at: https://www.euspa.europa.eu/newsroom-events/news-archive/space-enabler-security-and-defence (Accessed: 15 October 2024).

European Space Agency (ESA) (no date) 'The Zero Debris Charter', *ESA*, no date. [Online]. Available at: https://www.esa.int/Space_Safety/Clean_Space/The_Zero_Debris_Charter (Accessed 31 January 2024).

ESA (2023) 'Zero Debris Charter: Towards a Safe and Sustainable Space Environment', *ESA*, 2023. [Online]. Available at: https://esoc.esa.int/sites/default/files/Zero_Debris_Charter_EN.pdf (Accessed: 31 January 2024).

European Space Policy Institute (ESPI) (2020) 'Europe, Space and Defence. From "Space for Defence" to "Defence of Space"', *ESPI*, February 2020. [Online]. Available at: https://www.espi.or.at/wp-content/uploads/2022/06/ESPI-Public-Report-72-Europe-Space-and-Defence-Full-Report.pdf (Accessed: 31 January 2024).

Ferreira-Snyman, A. (2015) 'Selected Legal Challenges Relating to the Military Use of Outer Space, with Specific Reference to Article IV of the Outer Space Treaty', *Potchefstroom Electronic Law Journal*, 18(3), pp. 487–529; https://doi.org/10.4314/pelj.v18i3.02.

Fravel, M.T. (2015) 'China's New Military Strategy: Winning Informationized Local Wars', *China Brief*, 15(13), pp. 3–7. [Online]. Available at: https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/ (Accessed: 31 January 2024).

Freeland, S., Gruttner, E. (2020) 'The Laws of War in Outer Space' in Schrogl, K.U. (ed.) *Handbook of Space Security*. Cham: Springer, pp. 73–93; https://doi.org/10.1007/978-3-030-23210-8_59.

French Ministry for the Armed Forces (2019) 'Stratégie spatiale de défense, rapport du groupe de travail "espace"' [Defense Space Strategy, Report of the 'Space' Working Group], *Bureau des éditions*, July 2019. [Online]. Available at: https://www.vie-publique.fr/files/rapport/pdf/194000642.pdf (Accessed: 30 October 2024).

General Secretariat of the Council of the EU (2024) 'EU's Strategic Compass for Security and Defence: EU Publications', *European Council and Council of the EU*, 9 October. [Online]. Available at: https://consilium-europa.libguides.com/strategic-compass/EUpublications (Accessed: 31 January 2024).

Gerhard, M., Creydt, M. (2011) 'Safeguarding National Security and Foreign Policy Interests-Aspects of Export Control of Space Material and Technology and Remote Sensing Activities in Outer Space' in von der Dunk, F.G. (ed.) *National Space Legislation in Europe*. Leiden/Boston: Martinus Nijhoff Publishers, pp. 189–223; https://doi.org/10.1163/ej.9789004204867.iii-381.15.

Goswami, N. (2018) 'China in Space: Ambitions and Possible Conflict', *Strategic Studies Quarterly*, 12(1), pp. 74–97. [Online]. Available at: http://www.jstor.org/stable/26333878 (Accessed: 31 January 2024).

Harrison, T., Johnson, K., Roberts, T.G., Way, T., Young, M. (2020) 'Space Threat Assessment 2020', *Center for Strategic & International Studies*, March 2020. [Online]. Available at: https://www.csis.org/analysis/space-threat-assessment-2020/ (Accessed: 31 January 2024).

Hobe, S. (2019) *Space Law: A Handbook*. Baden-Baden: C.H. Beck; https://doi.org/10.5771/9783845266343.

House of Representatives (2023) '118th Congress 1st Session: To Amend Title 51, United States Code, to Update Government Oversight of Commercial Space Activities, and for Other Purposes', *House Committee on Science, Space, and Technology Republicans*, 1 November. [Online]. Available at: https://republicans-science.house.gov/_cache/files/5/4/54a60442-19b8-47ea-a21c-19b38c298d82/0260EA77510C0982D504F703238E205C.commercial-space-activities-xml.pdf (Accessed: 31 January 2024).

Jackson, N.J. (2019) 'Outer Space in Russia's Security Strategy' in Kanet, R.E. (ed.) *Routledge Handbook of Russian Security*. London: Routledge, pp. 227–238; https://doi.org/10.4324/9781351181242-22.

Jakhu, R.S., Jasani, B., McDowell, J.C. (2018) 'Critical Issues Related to Registration of Space Objects and Transparency of Space Activities', *Acta Astronautica*, 2018/143, pp. 406–420; https://doi.org/10.1016/j.actaastro.2017.11.042.

Johnson, C. (2018) 'Christopher Johnson' in Bragg, B. (ed.) *International Rules and Norms: Constraints on Space Operations: A Virtual Think Tank (ViTTa)® Report*. Boston: NSI Inc., pp. 14–15. [Online]. Available at: https://apps.dtic.mil/sti/pdfs/AD1095120.pdf (Accessed: 31 January 2024).

Kehrer, T. (2019) 'Closing the Liability Loophole: The Liability Convention and the Future of Conflict in Space', *Chicago Journal of International Law*, 20(1), pp. 178–216. [Online]. Available at: https://chicagounbound.uchicago.edu/cjil/vol20/iss1/5 (Accessed: 31 January 2024).

Khan, A.R. (2017) 'Space Wars: Dual-Use Satellites', *Rutgers Journal of Law and Public Policy,* 14(1), pp. 25–58. [Online]. Available at: https://rutgerspolicyjournal.org/2017/12/02/space-wars-dual-use-satellites/ (Accessed: 15 October 2024).

Klock, E., Aliberti, M. (2014) 'ESA Enlargement', *ESPI*, January 2024. [Online]. Available at: https://www.files.ethz.ch/isn/176962/ESPI_Report_47.pdf (Accessed: 31 January 2024).

Kopal, V., Neger, T., Walter, E., Kerrest, A., Stadlmeyer, S., Soucek, A., Mantl, L., Marboe, I., Fiorilli, S., Hobe, S. (2011) 'Outer Space – A Legal Issue' in Brünner, C., Soucek, A. (eds.) *Outer Space in Society, Politics and Law. Studies in Space Policy*. Vol. 8. Vienna: Springer, pp. 219–489; https://doi.org/10.1007/978-3-7091-0664-8_3.

Kozioł, S. (2022) 'Strategic Compass: Towards EU Space Strategy for Security and Defence', *Polish Institute of International Relations*, 24 January. [Online]. Available at: https://pism.pl/publications/strategic-compass-towards-eu-space-strategy-for-security-and-defence (Accessed: 15 October 2024).

Liu, H., Tronchetti, F. (2016) 'United Nations Resolution 69/32 on the "No First Placement of Weapons in Space": A Step Forward in the Prevention of an Arms Race in Outer Space?', *Space Policy*, 2016/38, pp. 64–67; https://doi.org/10.1016/j.spacepol.2016.05.004.

Lukowski, J. (2023) 'From Space Race to Disgrace: A Summary of the Russian Federation's National Space Legislation and its Recent Decline in the Global Space Sector (White Paper)', *Nebraska Law Review*, 2 May. [Online]. Available at: https://lawreview.unl.edu/Russian-Space-Law-Summary (Accessed: 15 October 2024).

Lyall, F., Larsen, P.B. (2018) *Space Law: A Treatise*. 2nd edn. London: Routledge; https://doi.org/10.4324/9781315610139.

Malinowska, K. (2017) *Space Insurance*. Alpen aan der Rijn: Wolters Kluwer International.

Maogoto, J., Freeland, S. (2007) 'Space Weaponization and the United Nations Charter: A Thick Legal Fog or a Receding Mist?', *International Lawyer*, 41(4), pp. 1091–1119; https://doi.org/10.2139/ssrn.1078405.

Messina, P. (2021) 'European Strategic Autonomy in Space, Through Space', *European Liberal Forum Policy Paper No 6*, June 2021. [Online]. Available at: https://liberalforum.eu/wp-content/uploads/2021/07/2021_06_10_Policy-Paper_N6.pdf (Accessed: 15 October 2024).

Mosteshar, S. (2019) 'Space Law and Weapons in Space', *Oxford Research Encyclopedia of Planetary Science*. [Online]. Available at: https://doi.org/10.1093/acrefore/9780190647926.013.74 (Accessed: 15 October 2024).

Mutschler, M.M. (2010) *Keeping Space Safe: Towards a Long-Term Strategy to Arms Control in Space*. Frankfurt: Peace Research Institute Frankfurt [Online]. Available at: https://www.jstor.org/stable/resrep14496 (Accessed: 15 October 2024).

National Aeronautics and Space Administration (NASA) (2023) 'Active International Agreements by Signature Date (as of September 30, 2023)' *NASA*, 30 September. [Online]. Available at: https://www.nasa.gov/wp-content/uploads/2023/10/house-approps-international.pdf (Accessed: 15 October 2024).

Pasco, X., Wohrer, P. (2023) 'Implementing the French Space Defence Strategy: Toward Space Control' *Fondation pour la Recherche Stratégique*, 30 June. [Online]. Available at: https://www.frstrategie.org/sites/default/files/documents/publications/notes/2023/202215.pdf (Accessed: 31 January 2024).

Peperkamp, L. (2020) 'An Arms Race in Outer Space?', *Atlantisch Perspectief*, 44(4), pp. 46–50. [Online]. Available at: https://www.jstor.org/stable/48600572 (Accessed: 31 January 2024).

Polkowska, M. (2022) *Eksploracja Kosmosu: Zagadnienia Prawno-Polityczne*. Warsaw: Instytut Wydawniczy EuroPrawo.

Preston, B., Johnson, D.J., Edwards, S.J.A., Miller, M., Shipbaugh, C. (2002) *Space Weapons Earth Wars*. Santa Monica, CA: RAND. [Online]. Available at: http://www.jstor.org/stable/10.7249/mr1209af.11 (Accessed: 15 October 2024).

Proelium Law (2023) 'Space Law in the UK' *Proelium Law LLP*, 15 May. [Online]. Available at: https://proeliumlaw.com/space-law-uk/ (Accessed: 31 January 2024).

Robinson, J. (2010) 'The Role of Transparency and Confidence Building Measures in Advancing Space Security' *ESPI Report 28*, September 2008. [Online]. Available at: https://www.files.ethz.ch/isn/124827/ESPI_Report_28_online.pdf (Accessed: 15 October 2024).

Rough, E., Kirk-Wade, E., Adcock, A., Housley, C. (2021) 'Future of the UK Space Industry', *House of Commons Library*, Debate Pack Number CDP 2021/0006, 3 February 2021. [Online]. Available at: https://researchbriefings.files.parliament.uk/documents/CDP-2021-0006/CDP-2021-0006.pdf (Accessed: 15 October 2024).

Sagath, D., Adriaensenb, M., Giannopapa, C. (2018) 'Past and Present Engagement in Space Activities in Central and Eastern Europe', *Acta Astronautica*, 2018/148, pp. 132–140; https://doi.org/10.1016/j.actaastro.2018.04.048.

Secure World Foundation (2023) *Pace industry statement in support of international commitments not to conduct destructive anti-satellite testing.* [Online]. Available at: https://swfound.org/industryasatstatement/ (Accessed: 31 January 2024).

SpaceWatch.Global (2019) 'European Military Space: Poland And USSTRATCOM Agree to Share Space Services and Data', *SpaceWatch.Global*, 16 April. [Online]. Available at: https://spacewatch.global/2019/04/european-military-space-poland-and-usstratcom-agree-to-share-space-services-and-data/ (Accessed: 15 October 2024).

Su, J., Lixin, Z. (2014) 'The European Union draft Code of Conduct for Outer Space Activities: An Appraisal', *Space Policy*, 30(1), pp. 34–39; https://doi.org/10.1016/j.spacepol.2014.01.002.

The National Archives (2021a) 'The Spaceflight Activities (Investigation of Spaceflight Accidents) Regulations 2021' Legislation.gov.uk, 2021. [Online]. Available at: https://www.legislation.gov.uk/uksi/2021/793/contents/made (Accessed: 15 October 2024).

The National Archives (2021b) 'The Space Industry (Appeals) Regulations 2021' Legislation.gov.uk, 2021. [Online]. Available at: https://www.legislation.gov.uk/uksi/2021/816/contents/made (Accessed: 15 October 2024).

Trautinger, M. (2016) 'The Impact of Technology and Export Controls on Small Satellite Missions' in Marboe, I. (ed.) *Small Satellites: Regulatory Challenges and Chances*. Leiden: Brill Academic Publishing, pp. 286–316; https://doi.org/10.1163/9789004312234_016.

Tronchetti, F. (2012) 'A Soft Law Approach to Prevent the Weaponization of Outer Space' in Marboe, I. (ed.) *Soft Law in Outer Space – The Function of Non-Binding Norms in International Space Law*. Vienna: Böhlau Verlag, pp. 361–386; https://doi.org/10.7767/boehlau.9783205791850.361.

Tronchetti, F. (2014) 'The Right of Self-Defence in Outer Space', *German Journal of Air and Space Law*, 63(I), p. 92.

Tronchetti, F. (2015) 'Legal Aspects of the Military Uses of Outer Space' in von der Dunk, F. (ed.) *Handbook of Space Law*. Cheltenham: Edward Elgar Publishing, pp. 331–381; https://doi.org/10.4337/9781781000366.00015.

Tronchetti, F., Liu, H. (2021) 'The 2019 Notice on Promoting the Systematic and Orderly Development of Commercial Carrier Rockets: The First Step Towards Regulating Private Space Activities in China', *Space Policy*, 2021/57, p. 101432; https://doi.org/10.1016/j.spacepol.2021.101432.

UK Ministry of Defence (2022) 'Defence Space Strategy: Operationalising the Space Domain' *UK Ministry of Defence*, February 2022. [Online]. Available at: https://assets.publishing.service.gov.uk/media/61f8fae7d3bf7f78e0ff669b/20220120-UK_Defence_Space_Strategy_Feb_22.pdf (Accessed: 31 January 2024).

United Nations General Assembly (UNGA) (1963) 'Question of General and Complete Disarmament A/RES/1884 (XVIII)' *United Nations Digital Library*, 17 October. [Online]. Available at: https://digitallibrary.un.org/record/203960?ln=en&v=pdf (Accessed: 15 October 2024).

Union of Concerned Scientists (2019) *UCS satellite database*. [Online]. Available at: http://perma.cc/C6M4-AWN2 (Accessed: 15 October 2024).

United Nations Institute for Disarmament Research (2022) 'Existing Legal and Regulatory Frameworks Concerning Threats Arising from State Behaviours with Respect to Outer Space', *UNGA*, 3 February. [Online]. Available at: https://documents.un.org/doc/undoc/gen/g22/248/57/pdf/g2224857.pdf (Accessed: 15 October 2024).

United Nations Office for Disarmament Affairs (no date) 'Treaty on the Prohibition of Nuclear Weapons' United Nations Office for Disarmament Affairs, no date. [Online]. Available at: https://disarmament.unoda.org/wmd/nuclear/tpnw/ (Accessed: 15 October 2024).

van Fenema, H.P. (2002) 'Launch Services and Satellite Export Controls: Recent Developments in the U.S.' in Böckstiegel, K.H. (ed.) *'Project 2001' – Legal Framework for the Commercial Use of Outer Space*. Cologne: Carl Heymanns Verlag, pp. 121–126. [Online]. Available at: https://d-nb.info/963630318/04 (Accessed: 15 October 2024).

Vidal, F., Privalov, R. (2023) 'Russia in Outer Space: A Shrinking Space Power in the Era of Global Change', *Space Policy*, in press, p. 101579; https://doi.org/10.1016/j.spacepol.2023.101579.

von der Dunk, F. (2021) 'Armed Conflicts in Outer Space: Which Law Applies?', *International Law Studies*, 2021/57, pp. 188–237. [Online]. Available at: https://digital-commons.usnwc.edu/ils/vol97/iss1/17/ (Accessed: 15 October 2024).

Weeden, B., Samson, V. (eds.) (2020) *Global Counterspace Capabilities Report*. Broomfield, CO: Secure World Foundation. [Online]. Available at: https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf (Accessed: 15 October 2024).

Willson, D.L. (2001) 'An Army View of Neutrality in Space: Legal Options for Space Negation', *Air Force Law Review*, 50(2), pp. 175–214.

Zahoor, S. (2017) 'Maintaining International Peace and Security by Regulating Military Use of Outer Space', *Policy Perspectives*, 14(2), pp. 113–135; https://doi.org/10.13169/polipers.14.2.0113.

Zelnio, R.J. (2007) 'Whose Jurisdiction Over the US Commercial Satellite Industry? Factors Affecting International Security and Competition', *Space Policy*, 23(4), pp. 221–233. https://doi.org/10.1016/j.spacepol.2007.09.011.

IV.4

MILITARY AND DEFENCE ISSUES OF DRONES AND ROBOTS

Chapter 12

Robots and Drones on Battlefields: New Capabilities and Emerging Challenges

Zvonko Trzun

Abstract

Recent armed conflicts have proved the undeniable value of systems commonly called robots or drones. The astonishing success of Azerbaijan in the 2020 Nagorno-Karabakh conflict, largely attributed to the strategic use of unmanned aerial vehicles (UAVs) by the Azerbaijani military, left experts and analysts in awe. However, the worth of UAVs had already been proven years earlier with the advent of the multi-role MQ-1 Predator.

This chapter provides a concise overview of UAV development, current capabilities, and potential future directions. The text is structured so that the first part describes the development of UAVs, and the second part focuses on unmanned ground vehicles (UGVs). The third part examines the extent to which Europe has embraced these new armed systems, analysing both European armed forces and industries – both striving to catch up with the main players in the unmanned vehicles market.

The chapter also describes the general shift in the world's security landscape, the rising sense of uncertainty, the long-forgotten fear of war, and the consequential surge in spending on military equipment. The development of artificial intelligence (AI) and the increasing autonomy of drones are briefly touched upon as this is an emerging field with the first AI-controlled systems still being tested. However, it is a topic deserving of a completely separate discussion. These points ultimately underscore the technical issues accompanying the usage of UAVs and UGVs, which occasionally lead to tragic errors. Whether the likelihood of such errors will decrease

Zvonko Trzun (2024) 'Robots and Drones on Battlefields: New Capabilities and Emerging Challenges'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 527–579. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_12

or increase as AI eventually replaces humans in controlling drones ("human out-of-the-loop") is likely to become evident in the very near future.

Keywords: drones, robots, unmanned aerial vehicles, unmanned ground vehicles, European military industry, artificial intelligence

1. Introduction

Analysing the increased use of robots and drones on modern battlefields, Colonel T. E. Hanson (at that time, director of U.S. Army Combat Studies Institute) said that they marked non-linear changes on the battlefields of the world.[1] Mathematically speaking, it would be correct to say that instead of linear growth, military capabilities experienced exponential growth, which physicists might call quantum leaps. Quite true, there are moments when breakthrough technologies have so strongly changed the previous balance of power that it is no exaggeration to say that nothing was the same thereafter. One such change was the discovery of gunpowder; another was the discovery of the atomic bomb; and the latest seems to be the introduction of autonomous unmanned weapons, the first technology to fundamentally affect not only the question of HOW wars will be fought in the future, but also WHO will fight in them.[2]

Going to war, or preparing for it, is not cheap. For example, the operational costs of military aircraft are staggering: In fiscal year 2018, a single B-2 Spirit bomber incurred expenses of 63 million dollars, flying a single F-22 Raptor fighter cost 22 million dollars, and flying the F-35, in one of its A/B/C versions, amounted to 13.4 million dollars. It is reasonable to assume these figures have significantly inflated due to rising costs in recent years. In stark contrast, unmanned weapons operate at a fraction of these costs.[3]

The advantages of robotic warfare are substantial. Robots respond to the increasing move to reduce human resources in the military. They accelerate operations, displaying unwavering focus and endurance without succumbing to human limitations like hunger, fear, or forgetfulness. Furthermore, robots possess capabilities that surpass those of humans: they can operate in radioactive environments, and they exhibit unparalleled precision in targeting (hitting a coin from 300 metres away, a feat beyond even the most skilled infantryman). Finally, robots will not hesitate to shoot to kill, a stark contrast to the moral dilemmas often faced by human soldiers.[4]

1 Doaré et al., 2014, p. 4.
2 Singer, 2009, p. 17.
3 McCarthy, 2020.
4 Tisseron, 2014, p. 5.

Experienced military leaders recognise the value of robots. General Rick Lynch, former commander of the U.S. Army's 3rd Armored Corps, commented on losing 155 men in combat. He asserts that 80% of those casualties were avoidable. There is no doubt in his mind: deploying a superior robot army could have saved 122 young lives in Iraq, which convincingly underscores the potential of unmanned weapons in mitigating human losses on the battlefield.[5]

2. Terminology Defined: Robots, Drones and Unmanned Vehicles

Although there is no shortage of definitions for the term "robot", there is no universally accepted definition. The ISO 8373:2021 standard states that a robot is a 'programmed actuated mechanism with a degree of autonomy to perform locomotion, manipulation or positioning'.[6] An additional note has been added, which states that a robot includes the control system. Autonomy is defined as the ability to perform intended tasks based on current state and sensing, without human intervention.

Another definition declares a robot to be a highly autonomous machine that '(1) senses, (2) thinks (in a deliberative, nonmechanical sense), and (3) acts'.[7]

The *Oxford English Dictionary* definition of a robot is: "a machine capable of carrying out a complex series of actions automatically, especially one programmable by a computer". In the book *Elements of Robotics*[8] the analysis delves deeper into this definition, particularly the phrase '…carrying out a complex series of actions automatically'. The phrase suggests that robots can perform tasks automatically, but it also emphasises that these tasks are inherently complex. For instance, anti-tank mines are not considered robots as they execute only a single action, even though they operate autonomously. Missiles are excluded from the category of robots for the same reason. The authors also highlight a pivotal characteristic of robots not explicitly stated in the Oxford Dictionary definition – the use of sensors. Simple machines cannot adapt their actions to their environment – but robots can, thanks to sensors.

Drawing from these elements, robots in this chapter are defined as machines equipped with sensors designed to perceive their environment; they can execute complex actions based on the perceived situation and are programmed to carry out these actions with varying degrees of autonomy. Unmanned vehicles are also types of robots, and depending on the domain, we divide them into aerial (UAVs), ground

5 Magnusson, 2010.
6 International Organization for Standardization [ISO], 2021.
7 Lin et al., 2008, p. 4.
8 Ben-Ari and Mondada, 2018, pp. 1–5.

(UGVs), surface (USVs), and underwater vehicles (UUVs). Some authors distinguish fixed-wing UAVs from rotary-wing UAVs, preferring the latter to be called drones. Considering that the term UAV is still more often used in professional literature, we also decided to give it priority.

3. Brief History of Unmanned Aerial Vehicles

The early application of modern military UAVs finds its roots in the development of the aerial torpedo in 1916. This groundbreaking weapon was engineered to target naval warships during World War I.[9] One of history's most renowned UAVs is the V-I flying bomb, also known as the "doodlebug", engineered in Nazi Germany. The V-I had an 848-kilogram warhead and was used during World War II. From June 1944 to March 1945, more than 9,000 V-I missiles were directed at England's territory.[10]

After World War II, research into UAVs continued, benefiting from significant advancements in automatic systems. In 1953, the Radioplane division at Northrop initiated the AQM-35 supersonic pilotless target aircraft. This aircraft had its maiden flight in 1956, achieving speeds of up to Mach 1.55. Its primary role was to assist in training the military to counter supersonic aerial threats.[11]

In the 1970s, Israel emerged as a leading manufacturer of UAVs, marking a significant era in the country's UAV development. Two standout UAV models during this period were the Mastiff and Scout. These drones played a crucial role in gathering intelligence, covering both ground and aerial surveillance of enemy forces, including precisely identifying radio locator locations and their parameters. They were also used in Israeli air strike operations. Their use extended to reconnaissance missions, to gather information on the effectiveness of these strikes, and to closely monitor the movements of enemy units.

After significant strides in UAV technology during the 1970s and 1980s, Israel ceded its leading position to the United States. The military conflicts of that era significantly shaped this transition in UAV leadership. In 1991, the United States launched Operation Desert Shield in Iraq in collaboration with its allies, attaining rapid success, which could be largely attributed to their cutting-edge technological capabilities. Subsequently, the Yugoslav War emerged as another significant conflict, where NATO and United Nations Member States jointly conducted Operation Deliberate Force in 1995. Reconnaissance assumed a central role in military planning during these conflicts, with military strategists drawing on the lessons gleaned from the Gulf War.

9 Ranquist, Steiner and Argrow, 2017, p. 1.
10 Sloggett, 2015, p. 24.
11 Palik and Nagy, 2019, p. 158.

Since the 1990s, UAVs have undergone a remarkable transformation, evolving into indispensable assets able to amass extensive data while operating at high altitudes over territories controlled by enemy forces.[12] Well before the onset of the War on Terror, the Central Intelligence Agency (CIA) already employed unmanned drones during the Bosnian conflict in 1994, operating under the classified designation of "Lofty View".[13]

The deployment of RQ-2 Pioneers by the Marines in Bosnia (1994) and Kosovo (1999), with launch operations conducted from the Ponce De Leon, marked notable instances of drone utilisation. Concurrently, the Hunter, a UAV jointly developed by Israel Aerospace Industries and TRW, was presented to the U.S. Army to fulfil its requirement for a short-range reconnaissance UAV. A substantial order of fifty Hunter drones, totalling $200 million, was delivered in 1993. However, the envisioned multi-billion-dollar programme faced eventual cancellation despite the Army, Navy, and Air Force all deploying Hunter drones. Designated as RQ-5A, the Hunter drones played a role in Operation Allied Force during the Kosovo conflict, amassing a cumulative flight time of 30,000 hours by 2004. This history of the Hunter underscores the long-term reliability of drones and highlights that armed forces were not fully ready to integrate them comprehensively.[14]

3.1. Predator: A Defining Milestone in UAV Technology

A more recent history of unmanned aerial vehicles will be illustrated through the most prominent UAV, General Atomics' Predator, along with its successors, the MQ-9 Reaper and MQ-9B Sky Guardian. However, large armed UAVs do not encompass the full spectrum of unmanned aircraft capabilities. UAVs have been designed in various sizes to cater to various tasks. They range from micro-drones weighing less than a kilogram, serving as surveillance tools to provide soldiers with a glimpse of what lies beyond the next wall, to giants weighing several tonnes, equipped with powerful missile systems capable of obliterating even heavily fortified enemy shelters.

The U.S. Military and NATO recognise three classes of UAVs: Class III includes aircraft weighing more than 600 kg, Class II are aircraft weighing 150-600 kg, and Class I includes the smallest unmanned aircraft. Class I drones are further divided into small, mini and micro UAVs. Normal deployment varies from tactical subunit for micro aerial vehicles to strategic and national employment for the largest UAVs.[15] The largest ones garner significant media attention, but a separate chapter could be easily written also for small drones, or for medium-sized ones.

In January 1994, the U.S. Department of Defense (DOD) finalised a contract with General Atomics to procure three systems, totalling ten aircraft, all based on the

12 Michel, 2013.
13 Shoker, 2021, p. 133.
14 Frantzman, 2021, p. 19.
15 NATO, 2019.

GNAT 750, a UAV that had previously been developed and utilised by the CIA. The new UAV was named the "Predator".

The Predator marked a significant milestone as the first medium-altitude endurance UAV created for the U.S. Air Force (USAF). Prior endeavours involving endurance UAVs, exemplified by the Compass Cope program, had focused exclusively on high-altitude endurance vehicles. The Predator's operational range extended between 3,000 and 25,000 feet, boasting impressive endurance, capable of remaining in flight for over 20 consecutive hours.[16]

Following the establishment of the Defense Airborne Reconnaissance Office, the inaugural operational utilisation of UAVs transpired in 1995. The USAF deployed its inaugural Predator unit, formally designated as the 11th Reconnaissance Squadron, to Bosnia in July of that year. This squadron fulfilled a pivotal role by furnishing indispensable aerial reconnaissance data until the conclusion of its mission in November. During this period, two Predators were lost – one due to enemy actions and another due to an engine malfunction.

Nevertheless, the surviving Predator was a crucial asset to NATO forces. The Predators communicated with ground pilots through a UHF satellite connection. This connectivity facilitated the transmission of real-time still images to ground terminals. The intelligence gleaned from the Predator's reconnaissance flights corroborated the violation of arms-removal agreements by several conflicting parties and contributed to identifying targets for an ensuing bombing campaign. This bombing campaign, in turn, played a pivotal role in compelling the warring factions to reengage in negotiations – which ultimately culminated in the signing of the Dayton Accord in 1995.[17]

3.2. Predator Transforms into a Multi-Role UAV

The USAF officially designated the Predator as the RQ-1. The Air Force employed the letter "Q" for designating unmanned aircraft dating back to World War II when the tradition began. In this context, the "R" denoted the aircraft's primary role in reconnaissance missions. When the Air Force employed a Predator aircraft to launch a Hellfire air-to-ground missile in 2002 (marking another pivotal moment in the platform's operational history), the UAV was again re-designated MQ-1 where "M" stands for "multi-role".

In the period spanning from June 2005 to June 2006, Predator UAVs were deployed on a total of 2,073 missions, accumulating an impressive 33,000 flight hours. During this time, they tracked 18,490 targets and executed 242 targeted attacks. These operational statistics reflect the Predator's strong performance during that particular period. As the utilisation of UAVs expanded, so did the demand for their services. By 2007, approximately 180 Predator UAVs were actively deployed, with multiple military units receiving approximately 300 hours of operational data

16 Blom, 2010, p. 92.
17 Ibid., p. 93.

and surveillance information from these aircraft daily. Although substantial, the available Predator fleet could not fully meet this high demand. These UAVs were primarily operated from the United States, yet they frequently launched their missions from locations near active war zones, as exemplified by their operations at Balad Air Base in Iraq. This strategic positioning allowed for swift and effective responses to emerging situations in conflict regions.[18]

As of September 2008, the United States Air Force had a total inventory of approximately 110 Predator aircraft (the number was constantly changing due to the poor reliability and frequent crashes of these aircraft). Predators played a pivotal role in the surge operations conducted in Iraq the same year, by providing an impressive 13,000 hours of video footage to ground troops every month. During this period, the Air Force conducted 24 simultaneous combat air patrol missions, ensuring continuous coverage. This remarkable operational intensity was possible because of a novel approach known as "split remote control". Under this framework, the take-off and landing phases were managed through line-of-sight control within the theatre of operations. Once the aircraft was airborne, control was seamlessly transferred to pilots located in the continental United States.[19] This innovative approach significantly expanded the pool of available pilots, resulting in an almost threefold increase in Predators operational at any given time. The utilisation rate increased from 30% to 85% of the overall inventory.[20]

A 2010 assessment of the drone inventory conducted by the U.S. DOD task force revealed there were 8,000 drones (large ones like MQ-1 Predators and MQ-9 Reapers, but also a great number of smaller UAVs), constituting 41% of the total military aircraft inventory. At that time, only a fraction of these drones – less than 1% – were equipped with weaponry. Their usage was still predominantly dedicated to intelligence, surveillance, and reconnaissance (ISR) missions.[21]

The inventory included 127 MQ-1 Predator, 31 MQ-9 Reaper, ten RQ-4 Global Hawk strategic reconnaissance aircraft, and various other UAVs serving diverse purposes. The Predator and Reaper UAVs could carry missiles, thus enabling new types of ground attack missions.

In addition to UAVs, the U.S. Army has deployed over 2,400 Talon unmanned ground vehicles (UGVs). These robots are equipped with cameras, motion sensors, and sound detectors and can operate day and night. They have robotic arms, flexible rotating shoulders, wrist and finger joints, and memory and learning capabilities. These attributes make them well-suited for reconnaissance within areas such as buildings, courtyards, sewers, and caves. Furthermore, they excel in the inspection of vehicles, removing roadblocks, and conducting border security patrols, among other functions.

18 Frantzman, 2021, p. 38.
19 Cuadra and Whitlock, 2014.
20 Blom, 2010, p. 108.
21 Frantzman, 2021, p. 23.

Modern armies were quick to recognise the growing importance and potential of unmanned military systems. For example, as early as 2009, the USAF had trained more pilots for UAVs than for traditional aircraft. By September of that year, 240 UAV pilots had graduated, outnumbering the 214 fighter pilots trained for manned aircraft. Although unmanned vehicles had yet to prove their worth in future conflicts (such as those in Nagorno-Karabakh or the Russo-Ukrainian war), this shift signalled an early indication of the approaching new era, with all the benefits and drawbacks that such a pivotal moment would bring.[22]

3.3. Poor Reliability of Predators

The MQ-1 Predator UAV is a weapon that has left a significant mark on military history, its success hard to dispute. Predators accumulated several million flight hours during their active service. Remarkably, while it took around fifteen years to accumulate the first million flight hours, the additional two million mark was reached in just two-and-a-half years, although this includes the hours accumulated by Predator's successor, the MQ-9 Reaper.[23] The Predator found its purpose and performed exceptionally well. In March 2018, USAF officially retired the MQ-1 Predator from operational service. A total of 268 Predators had been delivered to the service, of which just over 100 were still in service by the start of 2018.[24] The data on the small final number of active Predators provides one of the answers to the question – why would such a successful system be retired at all?

One of the reasons for the replacement was the appearance of the MQ-9 Reaper, a larger and more powerful UAV. Another reason pertains to the Predator's notorious unreliability. One report from 2014[25] revealed that from 2001, more than 400 large U.S. military drones had been involved in major accidents worldwide. Among these incidents, 194 drone crashes were categorised as Class A accidents,[26] indicating complete destruction of the aircraft or damages amounting to more than $2 million.[27] Military UAVs have occasionally landed on houses, farms, roads, or crowded areas. Sometimes, Predators and other UAVs behaved so unpredictably that pilots had to deliberately ram the drone into a mountain to avoid it falling into populated areas. In one notable incident, a UAV collided mid-air with a C-130 Hercules transport plane. One military UAV weighing approximately 150 kg fell near an elementary school playground in Pennsylvania, just minutes after students had left for home. Fortunately, no fatalities have occurred, but disasters have been only narrowly averted, often by a few feet. The list of incidents is extensive and several military drones have even vanished without a trace. Control over one armed Reaper was lost and it flew

22 Wu, 2022, p. 168.
23 Martin, 2013.
24 Donald, 2018.
25 Whitlock, 2014.
26 Gibb and Olson, 2008, p. 4.
27 Light et al., 2020, p. 2.

unguided across Afghanistan. Eventually, USAF fighters located and shot it down as it neared neighbouring Tajikistan.

Some accidents have occurred due to human error. For instance, in 2010, a Predator carrying a Hellfire missile crashed near Kandahar because the pilot failed to realise it was flying upside down. Certain human errors are caused by a lack of situational awareness of the ground control station (GCS). Unusual vibrations, noises, smells, and other sensory cues that a manned aircraft pilot would rely on are absent for a pilot situated thousands of miles away from a UAV.[28] To address this issue, General Atomics designed an enhanced GCS featuring high-resolution display that offers a 120° view, thereby improving the limited field of view (FOV) of a single-camera system.[29] Despite these enhancements, a UAV pilot cannot attain the same level of situational awareness as his counterpart in a manned aircraft.

Limited situation or operational awareness partially absolves the manufacturer of responsibility and should not impact the assessment of the aircraft's reliability. However, there are also numerous errors caused by technical problems. By 2014, almost half of all Predators had been involved in at least one incident – which explains why only around 100 Predators (out of the 268 purchased) "survived" their operational life.

Air Force officials acknowledged that Predators crash more frequently than regular military aircraft, but also claimed that the safety record of drones has improved considerably after the initial period of adjusting to the specific conditions of operating drones, which previously resulted in an extraordinarily high crash rate. For every 100,000 hours of Predators flown, there were 13.7 Class A accidents. Since 2009, this rate has dropped to 4.79 Class A accidents per 100,000 flight hours. However, this remained a very high accident rate, and therefore, most operators welcomed the new Reaper UAV that appeared in 2007.

Chris Cole from Drone Wars UK[30] (a site that follows the development of UAVs, but also the problems associated with their development) gives a somewhat discouraging diagnosis: 'Remotely controlled drones are inherently less safe than aircraft with a pilot onboard, and that is why we see so many crashes'. He sees more problems in the possibility that UAVs could be included in civil air traffic: 'While the military drone crashes that have happened so far tend to be in remote locations, if regulators give in to the increasing pressure to open up British and European airspace to these large drones, the impact is likely to be far greater'.[31] DOD officials have consistently defended the reliability of their UAVs – and yet, they have also admitted that this reliability can never match that of conventional aircraft with a pilot in the cockpit.

28 Gundlach, 2012, p. 674.
29 Jha, 2017, p. 65.
30 Cole, 2015.
31 BBC News, 2016.

3.4. MQ-9 Reapers: Bigger, Stronger, Even More Powerful UAVs

The success of the Predator fuelled a desire to develop an even more powerful UAV, equipped with a larger arsenal of weapons and capable of spending longer periods in the air, tirelessly hunting down the next potential target. The new UAV was based on the Predator, but with an increase in all dimensions: the wingspan was increased to 20 metres (14.8 m for the Predator), the length of the aircraft was increased to 11 m (8 m for the Predator) and it was equipped with a 950-shaft- horsepower/712 kW turboprop engine (a significant upgrade compared to the Predator's 115 hp/86 kW piston engine). The operational range has been increased to 1900 km, with an absolute ceiling of 50,000 ft. (15,420 m). Endurance is a staggering 27 hours or even 32 hours with additional external fuel tanks capable of holding 1,300 lbs of fuel. A particularly impressive leap forward has been achieved in terms of firepower. While later versions of the Predator could carry two AGM-114 Hellfire missiles, the Reaper can carry either eight AGM-114 Hellfire missiles or four Hellfire and two 500 lb (230 kg) GBU-12 Paveway II laser-guided bombs. The 500 lb (230 kg) of GBU-38 joint direct attack munition can also be carried.[32] However, this increased capacity comes at a price: the Reaper costs $32 million – eight times more than the Predator.

A Reaper system consists of three aircraft, a GCS, line-of-sight and a beyond-line-of-sight satellite and terrestrial data links, support equipment, personnel, and deployed crews, enabling 24-hour operations. Due to its impressive properties, it is on the wish list of many of the worlds' armed forces. In Europe, Belgium, Italy, France, Greece, Netherlands, Spain, and the United Kingdom have begun or already completed the procurement process.[33] Germany considered procuring Reapers, but eventually decided to lease the Israeli Heron UAV, while Finland and Poland recently announced their intention to purchase Reapers.[34]

The Reaper has been perfected based on lessons learned from extensive deployment of the Predator.[35] Additional valuable insights came from missions conducted using the Reaper, with the UAV being significantly enhanced from version to version. For example, the U.S. Navy asked for more range – quite understandable given its operations conducted across vast expanses of ocean. General Atomics responded by adding the additional external fuel tanks, a four-bladed propeller, engine alcohol and water injection, and elongated wings and tail surfaces as key upgrades. The new Reaper was 11.7 m long, and the wingspan was increased to 24 m. All these modifications have increased its endurance from 27 to 33–35 hours. The production designation of the new aircraft is Predator B/extended-range, although the name MQ-9B Reaper or simply Reaper ER appears more often in the media.

32 U.S. Air Force, 2021.
33 Gosselin-Malo, 2023; Kokkinidis, 2022; Stevenson, 2015.
34 Defense Industry Daily, 2023; Adamowski, 2022.
35 Gundlach, 2012, p. 18.

With its extended wingspan and increased range, the Reaper ER now meets the standards for civil aviation regulations. General Atomics CEO, Linden Blue, declared, '…the wing was designed to conform to STANAG 4671, and includes lightning and bird strike protection, non-destructive testing, and advanced composite and adhesive materials for extreme environments'.[36] Consequently, Reaper ER became the first medium-altitude long-endurance remotely piloted aircraft system (MALE RPAS) certified for operation within civilian airspace, complying with European flight regulations. No longer confined to military operations in conflict zones, Reaper transformed into an aircraft capable of long-term surveillance of civilian skies, able to undertake activities like border surveillance, search and rescue missions, anti-trafficking operations, and similar tasks. However, the MQ-9B SkyGuardian features weapons capability, harnessing the proven precision strike capacity of the MQ-9A Reaper. This Reaper variant is typically armed with 500-pound GBU-12 Paveway II laser-guided bombs and/or AGM-114 Hellfire missiles.[37]

Table 1. Comparison of MQ-1 Predator, MQ-9 Reaper and MQ-9B SkyGuardian (Reaper ER) characteristics.

	MQ-1 Predator	**MQ-9 Reaper**	**MQ-9B Reaper (ER)**
Introduced – Retired	1995-2018	2007	2016
Maximum Operational Altitude (ft)	25,000	50,000	45,000
Maximum Endurance (h)	24	27	> 40
Range (km)	1250	1900	2500
Maximum Take-off Weight (kg)	1020	4760	5670
Armaments	2xHellfire Missile	Combination of AGM-114 Hellfire missiles, GBU-12 Paveway II, GBU-38 Joint Direct Attack Munitions	Combination of AGM-114 Hellfire missiles, GBU-12 Paveway II, GBU-38 Joint Direct Attack Munitions
Price ($M)	4.5	30	32

36 General Atomics, 2016.
37 Attariwala, 2017, pp. 20–23.

The Reaper ER conducted its first operational flight in August 2015. Given that it will fly over civilian space, this certifiable Reaper was given the more appropriate name SkyGuardian or SeaGuardian, based on mission and payload. In 2016, the British Ministry of Defence (MoD) revealed that the extended-range version of the Reaper, the MQ-9B SkyGuardian, was selected for acquisition from 2018 to 2030.[38] In Britain, the aircraft will be called Protector. The new drone will be in service with the RAF from around mid-2024. An initial aircraft was handed over to the RAF in October 2022 but will remain in the U.S. for testing and training purposes. The USAF operated more than 300 MQ-9 Reapers as of May 2021, and it is still unclear how many UAVs the United Kingdom intends to order.[39]

The long-range capability of the SeaGuardian/MQ-9B Reaper is particularly attractive to countries with extensive maritime borders. For example, this issue is particularly important for the Indian Navy, because of the threat of Pakistani submarines. In 2023, India announced that it would begin the procurement of 31 MQ-9B Reapers in a contract worth 3.07 billion dollars. Indian officials and military leaders expect the procurement to significantly strengthen the Indian Navy's air anti-submarine warfare (ASW) capabilities. In keeping with the size of the oceans it oversees, the Indian Navy will receive 15 of the 31 new drones. Once India deploys the new MQ-9B Reapers, its Navy will become the second in the world (but certainly not the last) to conduct ASW operations using large UAVs.[40]

3.5. Reliability of the Reaper: Better than the Predator, Worse than Manned Aircrafts

But even as large UAVs become more powerful, they still have the problems of all new, under-tested systems that have been rushed to market. The new UAV MQ-9 Reaper is significantly more reliable than its predecessors, with 3.17 Class A accidents per 100,000 flying hours. However, this rate remains noticeably worse than manned aircraft; for instance, the F-16 fighter had a Class A accidents rate of only 1.96, while the F-15 had an even better rate of 1.47 accidents per 100,000 flying hours.

A good starting point for interested scholars is the Drone Wars UK site.[41] Their drone crash database is the result of methodical and persistent monitoring of USAF Accident Investigation Board reports, Wikileaks war logs, *The Washington Post* drone crash database, and general and military press reports. The site reports on crashes of large (Class II and III) military drones since early 2007.

For example, Drone Wars UK revealed that more than 400 large U.S. military drones were involved in major accidents worldwide from 2001–2014 (from a

38 Stevenson, 2015.
39 Insinna, 2021.
40 Haider, 2023.
41 Drone Wars UK, 2022.

comprehensive analysis conducted by *The Washington Post*).[42] Alongside the list of incidents, the main causes, referred to as 'fundamental safety hurdles' are outlined in the report as follows:

- Limited ability to detect and avoid trouble: Cameras and high-tech sensors on drones cannot fully substitute for a pilot's eyes and ears in the cockpit, leading to challenges in identifying and avoiding potential issues.
- Pilot error: Flying a drone is more complex than it appears, making human error a significant factor in accidents.
- Persistent mechanical defects: Some commonly deployed UAV models were designed without backup safety features and were rushed into service without extensive testing, leading to ongoing mechanical issues.
- Unreliable communications links: Drones rely on wireless transmissions for relaying commands and navigational information, but these connections can be fragile. In over a quarter of the worst crashes, communication links had been disrupted or lost, highlighting the vulnerability of drone communication systems.

Incidents involving large unmanned aircraft are particularly intriguing to the public and concealment of the details of such incidents is challenging. For instance, information about an MQ-9 Reaper that crashed into Lake Ontario during a training mission on November 12, 2013, was leaked to the public.[43] Although the Reaper was equipped with more safety mechanisms than its predecessors, these measures proved insufficient to save the malfunctioning UAV. According to the report, the drone's ground-based aircrew attempted to guide the Reaper back to base when it lost connectivity by switching to autopilot and charting a course back to base that avoided populated areas and potential obstacles. Another air crew attempted to connect with the drone, but a further global positioning system (GPS) and inertial guidance system error occurred. Within seconds, the drone initiated an automated right turn, causing it to invert and eventually enter into an unrecoverable spin.

Certain technical challenges are nearly insurmountable without a fundamental shift in design philosophy. The lightweight construction of the Reaper offers advantages, but it also makes the drone susceptible to strong winds, meaning that it must be grounded in adverse weather conditions. This poses a significant problem given that many missions occur over turbulent mountainous regions.[44] Additionally, there are other technical issues to consider. Older Reapers could not detect other aircraft, rendering them vulnerable to mid-air collisions. While the risk is relatively low when drones are flown over remote areas like Afghanistan, it significantly escalates if the Reaper operates over regions with heavy air traffic, such as Europe or the United States. It was not until 2019 that the introduction of a military Ground-Based Detect and Avoid Radar system at Syracuse International Airport allowed the Reaper to land and take off safely at this location. Before this

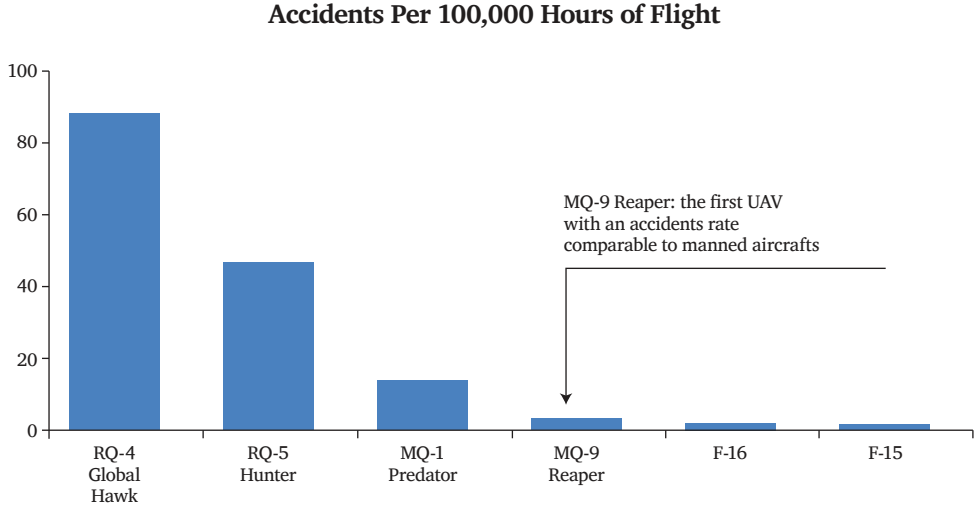
42 Whitlock, 2014.
43 Aegerter, 2013.
44 DoD Inspector General, 2020.

development, the MQ-9 had to be escorted by a manned civil air patrol aeroplane when ascending to and descending from altitudes of up to 18,000 feet.[45]

By early 2016, it was clear that the Reaper had persistent electrical problems. Problems with a faulty starter-generator caused the crashes or Class A accidents of 20 Reapers, half of which were in 2015 alone. Another early issue with the Block 5 aircraft, the newer generation of the Reaper, was that the avionics and other internal systems could not handle hot weather conditions. As a result, 2015 marked the worst year for drone crashes the USAF has ever had.[46] The problems were eventually solved by replacing critical components, after which the Reapers finally became more reliable.

Despite multiple problems, the latest General Atomics' unmanned aircraft demonstrate an above-average level of reliability, compared with earlier models. A 2005 U.S. DOD report[47] showed that in the late 1990s and early 2000s, UAVs were involved an unusually large number of Class A accidents, with a mishap rate (i.e., Class A accidents per 100,000 hours of flight) of 47 for the RQ-5 Hunter, 191 for the AAI RQ-7 Shadow and 281 for the AAI RQ-2 Pioneer. Even the largest UAV, weighing 14.6 tonnes and worth 130 million dollars, the Northrop Grumman's RQ-4 Global Hawk registered a mishap rate of 88, which is ten times higher than that of General Atomics' Predators and Reapers.

Figure 1: The accidents rate for the most used UAVs, compared with manned aircrafts



45 Olney, 2019.
46 Smith, 2016.
47 U.S. Department of Defense, 2005.

We have mentioned a large number of difficulties and incidents in this chapter – but maybe the picture is not so grim after all. Maybe UAVs were simply going through the development and testing stages that every other new product has to go through. The rapid decline in the number of accidents after 2015 suggests that the early 2000s represented what the 1900s were for manned aviation: a time of trial and error, constant learning, and countless lessons that this time (in the case of unmanned aviation) were not paid for in blood but only dollars.

In addition, it is crucial to recognise that not all UAV accidents are caused by technical failures; a significant portion can be attributed to the crews operating these systems. The role of an unmanned aircraft pilot is incredibly demanding, stressful, and often underappreciated. It is not surprising that they develop typical symptoms of post-traumatic stress disorder (PTSD), just like pilots who fly manned aircraft.[48] Confined, uncomfortable spaces and intensely concentrating on screens for hours, these pilots respond to constant inquiries from various agencies, analysts, troops, and, of course, commanders. The pilots receive fragmented information without context yet are expected to provide comprehensive real-time updates in return. One analysis succinctly captures the issue: 'Prior to drones, commanders relied on information flowing up the chain of command. Now they hunt for this information themselves, undermining the value of their own subordinates'.[49] Caught amidst conflicting directives from commanders at different levels of the chain of command, pilots strive to accommodate everyone, leading to stress, diminished concentration, and, ultimately, errors that can result in the destruction of the UAV.

3.6. What Is Next: The End of the Road, Or a Brand New Start for Reapers?

The U.S.AF announced their intention to upgrade the entire fleet, including 144 Block 1 and 136 Block 5 aircraft, to extended-range standards. These alterations are likely to be the final ones, as General Atomics is already developing the Reaper's successor, anticipated to be even more powerful, with an expected introduction in 2031. The end of service life of the MQ-9 fleet is scheduled for 2035.[50] But there is still no definitive decision, and the future of the Reaper appears uncertain at this juncture. The U.S.AF has been seeking approval to reduce its Reaper fleet from 351 to 276 aircraft by the end of fiscal 2023. Additionally, they propose halting the production of new Reapers entirely.

That strategic shift is likely influenced by information about new weapons developed by rival nations. The U.S.AF is concerned that Reapers could become vulnerable targets for Chinese air defences in a potential conflict. Given the substantial cost of each large UAV, such a scenario could be financially disastrous. Consequently, the Air Force is inclined towards developing smaller unmanned vehicles capable of

48 Werner et al., 2020, pp. 27–28.
49 McClure, 2015.
50 Insinna, 2021.

launching swarm attacks, thereby overwhelming enemy air defences at a reduced overall expense. Smaller unmanned aircraft can be very useful on the battlefield, using their small dimensions for easier survivability while performing reconnaissance missions, gathering information or directing artillery fire.[51] In light of this new strategy, there is diminishing room for Reapers, which cost tens of millions of dollars. Therefore, the Air Force hopes to retire more than half of the existing MQ-9 fleet by fiscal year 2027.

Advocates for continuing Reaper utilisation argue that the MQ-9 shares comparable survivability with other fourth-generation aircraft, indicating its potential to operate in threat environments akin to F-15s or F-16s.[52] The eventual outcome of this debate – whether supporters or staunch opponents of large, unmanned aircraft will prevail – remains uncertain. Some Reapers are scheduled to remain in service until 2035, although the exact number is unknown.[53]

UAVs must transition from being used to engage with poorly organised extremist organisations to operating in contested airspace. The initial upgrade will introduce a self-protection anti-jam antenna system, followed by the integration of new weaponry, an enhanced power system, and upgraded electro-optical and infrared systems.[54] Reapers must adapt to more formidable wartime conditions, or they risk vanishing from the skies permanently.

It is also possible that the Reaper will no longer be used as an independent hunter-killer, but instead, become a carrier of smaller UAVs. In recent years, the concept of a large unmanned aircraft acting as a mothership (central hub), bringing smaller UAVs closer to the target, has been explored. Discussion since 2020 suggest that the MQ-9 Reaper, or its upgraded version, the MQ-9B Sky Guardian, could potentially carry up to four smaller Sparrowhawks. The initiative, dubbed the Adaptive Airborne Enterprise (A2E), envisions an expanded role for MQ-9s. Under A2E, these aircraft would transcend their conventional functions and transform into mobile control hubs for a network of small drones and other systems. This network aims to establish an extensive sensing grid, facilitating target detection or establishing communication pathways for special operations forces operating deep within enemy territory.[55]

At present, this entire concept remains in the theoretical stage, much like the Sparrowhawk itself, which is still undergoing development. This compact unmanned aircraft system is designed as an "airborne launch and recovery demonstrator aircraft", meant to be carried and retrieved by a mothership, which could be either another larger drone or a different type of aircraft.[56] The benefit of employing compact, affordable, and disposable combat drones is clear: their capabilities, especially when

51 Bartulović et al., 2023, pp. 77–78.
52 Cohen, 2022.
53 Insinna, 2021.
54 Tirpak, 2021.
55 Roza, 2023.
56 Larson, 2020.

deployed in a coordinated swarm, could accomplish the desired mission objectives. All of this comes at a fraction of the cost of larger aircraft, and would not endanger the lives of pilots when used with a manned mothership.

3.7. More UAVs From Predator/Reaper Family

Several novel UAVs have been designed based on the architecture of the Predator and Reaper. While not all of them have been integrated into the Air Force or other military branches, they illustrate potential directions for UAV development in the near future:

- MQ-20 Avenger (formerly Predator C). Unlike the MQ-1 Predator and MQ-9 Reaper, the Avenger is powered by a turbofan engine. First launched in 2009, its design includes stealth features such as internal weapons storage and an S-shaped exhaust for reduced infrared and radar signatures. The Avenger is equipped with the same armament as the MQ-9. The jet engine allows it to fly at high subsonic speed (720 km/h), significantly faster than other UAVs from the same family: The maximum speed of the Reaper is 400 km/h, and the Predator flies at a mere 216 km/h. After testing, the U.S.AF decided that this platform still did not offer significant advantages over the MQ-9 Reaper, which they already had in service. The fact that the focus of operations at that time was Afghanistan, where the advantages of the Avenger did not come to the fore, probably contributed to the decision. However, in future, at least some UAVs will certainly follow the path of the Avenger: a jet engine will be necessary to achieve supersonic speeds and the possibility of fighting with manned fighters, while stealth characteristics will be a great advantage when the opponent uses the Anti-Access /Area Denial (A2/AD) strategy.
- Altair: this UAV is equipped with extra-long wings (wingspan is 26 m). It is powered by the same engine as the Reaper. The maximum altitude is an impressive 52,000 feet (16 km), and endurance is 36 hours. Today, these aircraft are used by NASA's Earth Science Enterprise, but it is conceivable that a similar design could be adopted by spy aircraft intended to collect data deep inside enemy territory.
- Mojave: this is a UAV with short take-off and landing (STOL) capabilities. Initially, the aim was to create a drone capable of vertical take-off and landing. However, this proved impractical as it required significant compromises in payload or endurance. Consequently, the focus shifted to a STOL design, ensuring optimal performance while requiring less runway space. Its configuration closely resembles that of the MQ-9 Reaper. Mojave successfully completed its inaugural test flight in the summer of 2021. In 2023, the UK announced its plans to acquire a Mojave system for trials aboard its Queen Elizabeth-class aircraft carriers. This UAV architecture is likely to be used in the future on aircraft carriers and elsewhere where take-off and landing space is limited.

4. When a 'Perfect' Machine Makes a Mistake: Civilian Casualties

As pointed out in Chapter 13, the use of UAVs is generally not controversial from a legal standpoint; however, a controversy arises in relation to the ways in which UAVs are employed. While it may be philosophically acceptable to excuse errors in armed systems by asserting nothing is perfect, such justifications lose credibility when faced with the most severe mistakes – those that lead to the loss of innocent human lives. UAVs have not been exempt from such errors, and it appears that, in numerous cases, the cause of fatal errors was the human factor.

In September 2023, *The New York Times* revealed that the final U.S. drone strike before the withdrawal of American troops from Afghanistan resulted in a tragic error, causing the deaths of 10 civilians, including seven children. Initially, the Pentagon denied this, but eventually, under mounting evidence, it had to acknowledge the accuracy of the newspapers' claims. The extensive investigation conducted by *New York Times* reporters showed that the U.S.AF had launched a Hellfire missile from an unmanned aircraft at an ordinary civilian vehicle. U.S. military officials attempted to defend their actions, claiming that the ground commander had compelling evidence to support the decision he had made. General Kenneth F. McKenzie Jr. (U.S.MC), Commander, U.S. Central Command, stated: 'At the time of the strike, based upon all the intelligence and reports we had, I was confident that the strike had prevented an imminent threat to our forces at the airport. Given that assessment, I and other leaders in the department consistently affirmed the validity of this strike'.[57]

U.S. military officials further attempted to bolster the legitimacy of their actions by pointing to a subsequent, larger blast that occurred in a nearby courtyard. However, upon inspecting the strike site, no evidence of a second, more substantial explosion was found. Despite their efforts to justify the incident, military officials were forced to abandon this last argument, subsequently suggesting that the second explosion might have been caused by a flare-up from a propane tank in the courtyard or perhaps the gas tank of a second vehicle in the area.[58]

The steadfast determination displayed by military officials in justifying their missile strike on an innocent man only raises more scepticism about the credibility of their claims. Their arguments, which bordered on the surreal, included labelling the driver as a terrorist merely for visiting a suspected Islamic State safe house (a claim later disproven), driving a white Toyota Corolla, and at one point loading something into the vehicle – an action that was carelessly and recklessly misconstrued as carrying explosives.

The MQ-9 Reaper, the UAV used for the attack, is equipped with the impressive Multi-Spectral Targeting System (MTS-B), featuring visual sensors for precise

57 U.S. Department of Defense, 2021.
58 Schmitt and Cooper, 2021, Section A, p. 1.

targeting. This system has an infrared sensor, colour and monochrome daylight TV cameras, shortwave infrared camera, laser designator, and laser illuminator. Full-motion video from each imaging sensor can be viewed as separate video streams or fused together.[59] However, even with this advanced technology, incidents can occur if the UAV is misused – or if commanders see only what they want to see.

Andrew Milburn, a retired Marine Corps colonel and former commanding officer of the Marine Raider Regiment and Combined Special Operations Task Force in Iraq, raises valid questions and provides answers in his insightful analysis: 'Anyone who has spent time in Afghanistan, indeed the Middle East, must be driven to question how "reasonable certainty" could be ascribed to a target description that loosely matched one in five vehicles on Afghan roads'. Mckenzie's statement reveals an opinion based more on wishful thinking than sound intelligence. When combined with high rank and a dominant personality, confirmation bias compounds initial errors, and causes other more junior but important participants in the process to be reluctant to challenge the views of a commander. The result is often what followed in this case – misidentification and tragic error.[60]

The incident on August 29, 2021 is a classic case of confirmation bias. This date marked the second-to-last day of the American forces' withdrawal from Afghanistan, a moment captured vividly in recent images: desperate individuals clinging to the wings and wheels of the final U.S.AF planes departing Kabul, now once again under Taliban control. General McKenzie reported more than 60 clear "threat vectors" indicating an imminent attack on Kabul airport. And only three days before, ISIS orchestrated a bombing that claimed 170 lives, including 13 American service members. The prevailing atmosphere was one of pervasive fear and uncertainty, with a pressing need to safeguard the lives of Afghan civilians and American soldiers.

But despite this tense environment, the unprovoked drone killing of an Afghan craftsman highlights the peril of wielding the lethal power of drones indiscriminately. This incident also raises a question – would the outcome have been the same if the decision had been in the hands of a pilot operating a manned aircraft? As Milburn perceptively observes, there is a prevailing, albeit implicit, notion that distancing human beings from such acts could somehow mitigate the moral weight of the act. At the same time, the U.S. President fostered the misconception that drones are more precise and less harmful to non-combatants. This notion is completely misguided, rooted in an overreliance on technology coupled with wishful thinking. The stark truth remains: drones are thirty times more likely to cause civilian casualties compared to manned aircraft.

For more than two decades, the problem of civilian casualties resulting from drone strikes has arisen persistently in conflicts in regions like Afghanistan and Iraq. In December 2013, a tragic incident occurred when the USAF targeted a convoy of 11 cars and pickup trucks in rural Yemen with four Hellfire missiles. Initially,

59 U.S. Air Force Website, 2021.
60 Milburn, 2021.

both the Yemeni authorities and the U.S. government labelled the victims as terrorists, claiming the operation had targeted a high-ranking member of Al-Qaeda in the Arabian Peninsula. However, it was later revealed by witnesses and relatives that the victims were actually part of a wedding procession.[61]

This incident is just one among many misdirected strikes. Independent estimates from non-government organisations, New America and the Bureau of Investigative Journalism, indicate that civilians accounted for 7.27% to 15.47% of deaths in the U.S. drone strikes in Pakistan, Yemen, and Somalia from 2009 to 2019.[62] The same organization reported hundreds of civilians killed.[63] Unfortunately, this issue is unlikely to be resolved soon as the Washington administration maintains its focus towards what officials refer to as "over the horizon" operations in Afghanistan – strikes conducted against terrorist targets in countries at a considerable distance from ground control.[64]

The initial step in preventing future mistakes involves acknowledging responsibility and thoroughly analysing the reasons behind the error. However, there is little optimism that the U.S. Military will exercise more caution in approving new strikes on alleged terrorists. A mere two months after the Kabul incident came to light, Pentagon inspectors concluded their investigation, stating that the U.S. UAV strike that claimed the lives of 10 Afghan civilians was an error, albeit not a violation of any laws. USAF Inspector Lieutenant General Sami Said informed reporters, 'It was an honest mistake',[65] leaving them to speculate on the exact implications of such phrasing and why those responsible for an "honest mistake" are not held accountable.

What is unequivocal, however, is that the MQ-9 Reaper and Hellfire missile it deployed functioned flawlessly. Yet, given that the use of these exceptional weapons can swiftly lead to catastrophic consequences, it is evident that unmanned weapons, or at least their distant pilots, are not yet prepared to operate over civilian populations or to be used for tasks such as border surveillance and similar law enforcement activities.

4.1. Reaper's Potential Flaws: Technology in Focus

We have established that the equipment installed in the Reaper UAV represents the top available technology, including the MTS-B EO/IR (Multi-Spectral Targeting System) that combines electro-optical/infrared, laser designation, and laser illumination capabilities in a single sensor package. This system for Reapers is supplied by Raytheon. According to General Atomics, the Reapers are equipped so that they

61 Human Rights Watch, 2014.
62 Grossman, 2019.
63 Gittins, 2020.
64 Milburn, 2021.
65 Schmitt, 2021, Section A, p. 1.

deliver the best image to the pilots, and there is even a ground/dismount moving target indicator to help pilots with the automatic identification and tracking of the target:

> GA-ASI's Lynx Multi-Mode Radar is a high-performance system that provides high-resolution, photographic-quality imagery that can be captured through clouds, rain, dust, smoke and fog… Integrated into USAF MQ-9 Reaper RPA, the DMTI mode allows pilots to detect slow-moving, operationally significant personnel or vehicles. In addition, pilot can select a GMTI/DMTI target and automatically cross-cue to the EO/IR sensor in narrow FOV for visual identification of the target.[66]

In other words, the Reaper ensures clear images without interference from clouds or smoke when transmitting to the GCS. The system automatically tracks the targets, revealing their location and where they hide. But can this be entirely trusted?

4.2. Poor Image Quality

In a New York Times article (written by the same journalist who revealed the story to the U.S. public, and then to the whole world), scenes filmed during the disastrous Reaper attack on civilians on August 29, 2021, are described as "murky"; later journalists write about "blurry images" or "blurry footage". Actually, the word "blurry" is mentioned six times.[67] If Reaper's pilots and their commanders really had to decide whether to launch an attack based on such poor-quality footage, could they even have made a better decision? The MQ-9 Reaper does have the higher-resolution colour camera, but it seems that it was used too little or too late on this occasion.

The second article[68] highlights numerous errors made by USAF unmanned aircraft pilots, including the July 2016 incident when what were thought to be three ISIS staging areas on the outskirts of Tokhar, northern Syria were targeted. The Pentagon reported 85 enemy fighters killed. However, the reality was very different: U.S. missiles struck houses far from the front line, where farmers, their families, and other local residents sought refuge from nightly bombings and gunfire. Tragically, over 120 villagers lost their lives in the attack. The article mentions the promises made by U.S. military officials regarding the enhanced "over the horizon" long-range surveillance capabilities of UAVs. In stark contrast, multiple official reports highlight shortcomings in both the quality and quantity of video footage, which ideally should form the basis for targeted attacks with minimal collateral damage.

In some instances, the issue was not just the quantity of the video but also its quality. Analysts at the military's Combined Air Operations Center in Qatar encountered this challenge when they examined 17 minutes of unclear footage preceding

66 General Atomics, 2020.
67 Savage et al., 2022, Section A, p. 1.
68 Khan, 2023.

a strike on an ISIS "defensive fighting position" in Ramadi on November 13, 2015. Upon further review, they determined that what was initially identified as an 'unknown heavy object' being moved into a building was, in fact, 'a person of small stature', resembling 'how a child would appear standing next to an adult'.[69]

Accurately identifying the enemy is a fundamental aspect of the targeting process. However, there have been several cases where ordinary citizens were mistakenly identified as combatants. While we are on the subject, the Pentagon presents disproportionately low figures regarding misidentification. Their official records indicate that misidentification occurred in just 4% of cases. However, during visits to incident sites conducted by The New York Times, misidentification played a significant role in 17% of cases, contributing to almost a third of civilian deaths and injuries. Why is this happening? After all, the prerequisites for precision strikes seem to have already been achieved. The weaponry carried by the MQ-9 Reaper has already been rigorously tested. The systems have been constantly upgraded over the years, and they proved their worth in the 1991 Persian Gulf War, in NATO's 1999 campaign in the Balkans, in Yemen and Somalia. This applies both to the Reaper Multi-Spectral Targeting System and also to the laser guidance of Hellfire missiles. So when the weapon is already so perfected, it should be utilised appropriately: after the Trump administration came to power, the pace of using powerful UAVs was significantly accelerated. American forces have executed more than 50,000 airstrikes in Iraq, Syria, and Afghanistan. Trump also gave the CIA the authority to conduct drone strikes; that decision is discussed in Chapter 13, where CIA operations are aptly characterised as having a "clandestine nature". All of this obviously suggests a rising trust in unmanned weapons, a trust that is largely justified, but occasionally still excessive.

4.3. Laser Guidance, Known Issues

Excessive confidence arises because the subpar quality of the video is not the only critical aspect of the technology in use. The MQ-9 Reaper employs two types of ammunition: the AGM-114 Hellfire guided missile and GBU-12 Paveway II bombs (where "GBU" stands for "Guided Bomb Unit"). Both weapon systems are laser-guided. The sensor operator, stationed alongside the pilot in the GCS, utilises a laser targeting marker to "paint" the target, a task that can also be performed by ground troops in conventional combat zones. The challenge with this type of guidance lies in its susceptibility to being compromised by clouds, smoke, fog, or dust. This is precisely why many militaries resort to GPS-guided weapons. The GPS guidance may be less precise, but it will not be affected by unfavourable environmental conditions.

However, even if we presume the weapon operates optimally – with flawless video quality enabling target display, seamless functioning of the Ground/Dismount Moving Target Indicator allowing automatic target identification and tracking, and

69 Ibid.

impeccable performance of Reaper's missiles and bombs that accurately follow the designated laser beam – the reality is that the operation of large UAVs is still far from the promised 'putting warheads on foreheads'.[70] This phrase should signify the UAV's ability to hit its target with surgical precision, minimising, and perhaps even eliminating collateral casualties.

Undoubtedly, the Hellfire missile has achieved remarkable accuracy and precision. In external ballistics, "accuracy" denotes the alignment of the mean impact point with the target position, whereas "precision" refers to the dispersion of impact points.[71] Low accuracy typically results from systematic deterministic errors, while low precision arises from non-deterministic errors, such as deviations in the thrust force direction from the missile's longitudinal axis of symmetry, errors occurring during missile production, and unpredictable sudden changes in wind, among others.[72] The accuracy of the Hellfire is satisfactory, and its Circular Error Probable (CEP) is among the smallest in its class of laser-guided missiles. According to the DOD Dictionary of Military and Associated Terms, CEP is "an indicator of the delivery accuracy of a weapon system, used as a factor in determining probable damage to a target. It is the radius of a circle within which half of a missile's projectiles are expected to fall".[73]

4.4. A Misalignment of Purpose: The Anti-Tank Weapon in the Wrong Role

Therefore, accuracy should not be the primary concern, even in (moderately) unfavourable conditions. The real issue lies in the Hellfire's lethality. Originally designed as an anti-armour missile, its "kill zone" extends up to 15 metres and has an "injury radius" of 20 metres. This means that any inadequately shielded target within 20 metres of the Hellfire's impact site will sustain severe injuries, and a significant number of enemies (but also innocent bystanders) may be fatally wounded.[74] Such a projectile can hardly be deemed as having a "selective effect"; expecting the target to be isolated and at least 20 metres away from everybody else is highly unrealistic, especially in conditions of urban warfare.

The pursuit of "winning hearts and minds" seems to ignore this inherent logical flaw. To satisfy global public opinion, public relations services tend to promote what former USAF officer Peter Goodrich, in his yet unpublished but extensively cited discussion, dubs 'the surgical precision myth'.[75] This myth concerns the illusion that only "bad guys" will be struck by smart ammunition, sparing civilians. In fact, the prolonged use of cutting-edge weapon systems – updated UAVs, skilled crews, and state-of-the-art laser-guided missiles – demonstrates that even this combination

70 Mulrine, 2008, p. 45.
71 Wall, 2013.
72 Trzun et al., 2021, pp. 18–19.
73 U.S. Department of Defense, 2011.
74 Chamayou, 2015, p. 199.
75 Goodrich, 2003.

cannot guarantee that only individuals positively identified as terrorists or enemies will be targeted.

Some authors assert that smart munitions are not designed to safeguard civilian lives but merely to advance the political and economic interests of the entities deploying such missiles. They concede, however, that abandoning the practice of "carpet bombing" (employed until the advent of smart ammunition, even in wars of the 1980s) significantly reduced civilian casualties. The use of smart ammunition also has additional advantages, including cost reduction due to fewer sorties required, a reduction in hostilities from nations where air operations are conducted, and increased protection for one's own pilots and troops involved in combat.[76]

From an engineering perspective, the combination of the MQ-9 Reaper UAV and smart ammunition like the AGM-114 Hellfire represents perhaps the most viable solution at present, especially in regions where air superiority has been established (the UAV's ability to counter modern manned aircraft will be discussed later). Unfortunately, it remains imperfect at present. This is to be expected given that it carries a warhead weighing 8-9 kg, whose impact cannot be confined to just one individual.

The new ammunition set to replace the Hellfire, the AGM-179 Joint Air-to-Ground Missile, incorporates a tri-mode seeker featuring a low cost imaging sensor, Semi-Active Laser sensor, and Millimeter Wave (MMW) sensor. While this developmental direction will undoubtedly enhance target tracking, the missile's substantial warhead mass suggests that the issue of collateral victims will remain unresolved.

4.5. Human Error

The risk of human error has been constantly reduced. However, it seems that despite the many improvements made in the last three decades, there is still room for improvement in the quality of the technology of large UAVs and their weaponry, and the existence of these technological limitations do not completely remove the burden of guilt from the personnel involved. Today, operating UAVs is accompanied by high levels of responsibility, and the process of approving an individual attack is rigorous and complies with the law of armed conflict (the legal basis is explained in Chapter 13, with a particular distinction between "old" and "new" weapons). To deploy the selected missile, clearance from both the mission commander and military lawyer must be obtained before the sensor operator guides it to the target and the pilot fires the missile. In accordance with these refined procedures and all technological advancements, one can expect the future will bring the most precise and transparent air campaign ever. However, investigations by journalists and non-government organisations seem to present a different reality, particularly in cases where mistakes lead to unintended civilian casualties.

After the August 2021 incident in Kabul, Cpt, Bill Urban, spokesman for the U.S. Central Command, said that 'even with the best technology in the world, mistakes

76 Herold, 2008, pp. 96–99.

do happen, whether based on incomplete information or misinterpretation of the information available. And we try to learn from those mistakes'. He also admitted that confirmation bias is a genuine concern and emphasised the need for further efforts to address this issue. Indeed, he specified that the fight against errors (caused by technological or human flaws) is still far from over.

Large UAVs are extremely complex weapon systems, involving the UAV's video and targeting sensors, missiles equipped with precise laser designation, and the proficiency and judgement of the pilot and commander. However, it appears that there are instances where at least one component of this system fails, resulting in tragic consequences. Unfortunately, at this point, a single error within only one component of these highly complex systems is all it takes to create the conditions for tragedy, especially given the absence of an adequate backup in technology and procedures.

Some authors argue that even modern UAVs like the MQ-1 Predator or the MQ-9 Reaper are not autonomous or robotic platforms since they are operated by human controllers in real time.[77] They are classified as robots due to their ability to perform autonomous actions, such as patrolling above designated areas or returning to base when communication with the GCS is lost. Although they require pilot confirmation to launch a missile, this necessity primarily arises from safety and legal concerns rather than the UAVs' inability to conduct strikes autonomously. Unfortunately, it is now clear that keeping "the human in the loop" (the concept is further explained in Chapter 13) does not completely eliminate the possibility of tragic errors.

4.6. Issues Caused by Enemy Electronic Warfare

The use of unmanned vehicles introduces a certain risk because there is no pilot/operator to correct and halt unforeseen movements, and unforeseen incidents are quite possible in the event of a communication breakdown with the remote pilot.

Best lessons related to deployment of unmanned vehicles come from the conflict in Ukraine. Initially, the Ukrainian Army managed to partially compensate for a manpower shortage and less advanced equipment by employing robots and drones. Unmanned aircraft, in particular, posed problems for the Russians, with UAVs constantly flying across the sky, collecting data, directing artillery fire, and even attacking Russian vehicles and infantry. However, it appears that, after the initial shock, the Russian Army managed to regroup. A comprehensive summary from November 2023 encapsulates it all most effectively:

> Ukrainian and Russian forces continue to grapple with the challenges electronic warfare (EW) systems pose on the front. The Economist reported that superior Russian EW systems are impeding Ukrainian reconnaissance, communication, and strike capabilities. The Economist, citing Western experts, stated that Russia has placed a "huge focus" on producing and developing superior EW capabilities and that

77 Jha, 2017, p. 224.

> Ukraine is struggling to produce equivalent EW systems and EW-resistant weapons domestically.[78]

According to General Valery Zaluzhny, the commander-in-chief of the Ukrainian Army, their forces initially faced weak electronic warfare (EW) capabilities from the Russians. This allowed them to utilise unmanned weapons, primarily aerial and occasionally floating drones, to a significant extent. However, the Russians quickly bolstered their EW systems, deploying them extensively along the entire frontline. These are no longer outdated Soviet-era systems but modern setups capable of disrupting drone communication with control stations, often determining the location of Ukrainian remote pilots and redirecting artillery fire accordingly. Even modern Western missiles like Excalibur or High Mobility Artillery Rocket System (HIMARS) started experiencing accuracy issues due to Russian jamming.

Where do Russia's unexpectedly advanced EW capabilities originate? After facing setbacks in electronic warfare during the 2008 Russo-Georgian War, Russia shifted its focus to enhance capabilities in the electromagnetic spectrum. The shortcomings became apparent as Russia's EW proved inadequate in suppressing Georgian air defences, providing cover for advancing forces, and establishing effective jamming zones. These failures acted as a wake-up call for Russia, prompting an acknowledgement of deficiencies within its forces and their deployment.[79]

Moscow embarked on an ambitious programme to reform and modernise its military forces. A commitment was made to achieve a target of 70% new or modernised military inventory. Thereafter, many observers and defence officials asserted that Russia's prowess in EW surpasses that of Western countries. Russia places a significant focus on EW due to its cost-effectiveness in diminishing the capabilities of adversaries. While NATO countries boast modern military systems that Russia may find unaffordable or technologically inaccessible, EW allows Russia to effectively counter nearly all that NATO currently possesses.[80]

EW is assuming a growing and essential role, rightfully earning its status as a force multiplier. This is evident in Russia's daily demonstrations on the battlefields in Ukraine. The present-day Russian military exhibits substantial strength compared to the Soviet military in the 1990s. It is plausible that the effectiveness of the Russian military against weapons sent by the West to aid Ukraine is, in part, attributed to its formidable EW capabilities.

Systems like RB-341V Leer-3, R-330Zh Zhitel, 1RL257 Krasukha-4, and others perform their designated tasks with notable success, including jamming communication signals, transmitting false GPS signals, and employing various methods to execute the three primary operational functions of electronic warfare:

78 Evans et al., 2023.
79 Smith, 2020, p. 2.
80 Ibid., p. 5.

- Electronic Attack, which encompasses jamming. In this context, a transmitter overwhelms or disrupts the waveform of a hostile radar or radio.
- Electronic Support, involving surveillance and warning information derived from intercepted electromagnetic emissions.
- Electronic Protection, offering protection to the host platform against electronically controlled threats.[81]

Ukraine is countering Russian EW measures with quantity, having trained approximately 10,000 drone pilots who constantly strive to identify vulnerabilities in the heavily fortified Russian EW defence. The Ukrainians rely on quantity, modifying inexpensive commercial drones to exploit weaknesses in Russian defences. However, these budget-friendly drones have a significant drawback – susceptibility to jamming. It is estimated that as a result, Ukraine loses up to 2,000 drones per week. Their communication with control stations is disrupted, leading them to aimlessly roam the sky until their batteries deplete, after which they fall to the ground. Although autonomous systems governed by AI might overcome such countermeasures, this option is currently not feasible, at least not for mini-drones that Ukrainians use.[82]

A particular issue is the ability of Russian EW forces to swiftly and accurately locate the source of electromagnetic (EM) radiation emanating from Ukrainian forces. On Ukraine's battlefields, the simple act of powering up a cell phone can attract enemy artillery fire. The same holds true for Ukrainian artillery radars and remote-control stations for UAVs.[83] Consequently, sending drones has become a perilous activity carried out only from well-established cover. Ukrainian pilots sadly remark that they once could operate their aircraft from considerable distances, but now they must approach almost to the front lines of the Russian forces. UAVs have a very limited time to reach an enemy target and launch an attack before they are disabled by EW measures.

The U.S. DOD is actively seeking ways to minimise civilian casualties resulting from U.S. military operations. In 2022, they introduced the Civilian Harm Mitigation and Response Action Plan (CHMR), aiming to identify and implement necessary measures. Some of these measures can be swiftly put into action, for instance: 'Combatant commands [will] identify and incorporate CHMR lessons learned and recommendations into current joint targeting processes to reduce the risk of civilian harm in future operations.'.[84] Further, it is essential to enhance situational awareness, and understand the local population behaviours. Based on past negative experiences, the focus now is on implementing practices to gain information about civilians and civilian objects across the joint targeting process. This includes details about civilian

81 McDermott, 2017, pp. 15–28.
82 The Economist, 2023.
83 Stashevskyi and Bajak, 2022.
84 U.S. Department of Defense, 2022, p. 12.

patterns of life, population density, and infrastructure, which is vital for civilian health and safety.

The Under Secretary of Defense for Acquisition and Sustainment, in collaboration with the Under Secretary of Defense for Research and Engineering, is tasked with updating the DOD Standard Practice System Safety. This update includes 'incorporating features into system safety reviews for future weapon systems that support civilian harm mitigation objectives, such as render safe, pre-planned post-launch abort, and scalable yields'.[85]

As mentioned earlier, it appears that the new AGM-179 (JAGM) program does not currently focus on reducing the likelihood of collateral casualties. While there is a heightened emphasis on enhancing weapon efficiency, it is possible that the new guidelines might bring significant changes in this regard as well.

4.7. UAVs Engaged in Direct Combat Against Manned Fighters

Today, UAVs are achieving remarkable success and ever increasing reliability in their operations, as illustrated in Figure 1. Although their primary functions have historically centred on reconnaissance and surveillance, a significant shift is underway. These UAVs are progressively moving into domains traditionally exclusive to manned aircraft. For instance, the MQ-9 Reaper has assumed the role of a hunter-killer, the MQ-20 Avenger has emerged as one of the pioneering jet UAVs, and the Boeing MQ-25 Stingray stands as the premier aerial refuelling drone. This trend signals a transformative era where UAVs are expanding their operational scope beyond previous limitations.

The next inevitable step is confrontations between UAVs and manned military aircraft. In this imminent clash, UAVs may be guided by remote pilots or operate autonomously, driven by embedded AI.

However, current UAV technology is not fully prepared for this face-off. UAVs manufactured by General Atomics are engineered to be lightweight, with highly efficient engines, and wings designed to generate adequate lift even at low speeds. The challenge in wing construction lies in achieving the optimal drag/lift ratio under anticipated operational conditions. Unlike modern manned fighters equipped with delta wings that offer relatively low resistance at supersonic speeds while ensuring sufficient lift, UAVs have wings swept at very low angles. These long, slender wings give UAVs a resemblance to gliders rather than traditional manned fighters – but such construction grants them extended endurance and ample lift at low speeds.[86]

Resolving conflicting criteria within a single design is a challenge. Consequently, current UAVs remain tailored for prolonged, slow flight, prioritising endurance over high speeds or abrupt manoeuvres. Even advanced jet-powered models like the

85 Ibid., p. 13.
86 Gundlach, 2012, p. 374.

MQ-20 Avenger were rejected by the USAF due to their unsuitability for surveillance and counter-terrorism missions.

In March 2023, a significant event highlighted the limitations of lightweight UAVs designed for prolonged flight. This incident confirmed what was already anticipated: in a direct confrontation, UAVs stood little chance against manned aircraft. A declassified video released by the U.S. European Command captured the moment when two Russian fighter jets aggressively approached a U.S. drone flying over the Black Sea, clearly intending to expel it from the area. If the UAV did not alter its course immediately, the Russian jets openly threatened to attack it and bring it down.[87] While the UAV was flying at about 25,000 feet, two Russian Su-27 fighter jets made 19 high-speed passes near the Reaper.

The attack, executed by a Russian Su-27 fighter, lasted approximately 30 to 40 minutes. The MQ-9 Reaper UAV's rear-facing camera recorded the tense encounter, revealing the Russian Sukhoi fighter approaching and, just before the UAV passed over, releasing fuel onto the U.S. Reaper. Despite the unexpected impact, the UAV maintained stability and continued its flight. In a subsequent pass, the Russian jet repeated the manoeuvre, dumping fuel as it neared the UAV. The video feed from the UAV was then disrupted as the Russian fighter collided with the MQ-9 Reaper, causing damage to the propeller and compelling the U.S. forces to bring down the drone in the Black Sea.[88]

The Kremlin denied any collision, while the Pentagon acknowledged the physical contact, diplomatically suggesting it might have been an unintended mistake by the Russian pilot. This incident underscored the vulnerability of lightweight UAVs in direct encounters with manned military aircraft. The incident was not the first of its kind, and it certainly will not be the last. In July 2023, a Russian fighter jet flew "dangerously close" to a U.S. drone over Syria. During the last pass, the Russian manned aircraft deployed a flare that severely damaged the Reaper's propeller and forced it to return to its home base.[89] It seems that the Russians have found an efficient way to eliminate unwanted surveillance UAVs from their area of interest without resorting to an overt attack that could provoke a strong reaction from the other side.

'The Russian fighter's blatant disregard for flight safety detracts from our mission to ensure the enduring defeat of ISIS', said the Air Force Central Command[90] – but as far as their reaction is concerned, everything is left to verbal condemnation. Currently, their UAVs cannot compete with enemy fighters in any way. Lacking robust self-defence mechanisms and possessing highly restricted manoeuvrability, UAVs are akin to "sitting ducks", relying solely on the hope that they will not draw the attention of vastly superior manned aircraft.

87 Olson and Chappell, 2023.
88 Schmitt and Cooper, 2023, Section A, p. 7.
89 Breen, 2023.
90 Liebermann, 2023.

Engineers from General Atomics attempted to give their UAVs a chance to fight back. Shortly before the start of Operation Iraqi Freedom, several MQ-1 Predators were armed with AIM-92 Stinger air-to-air missiles to deter Iraqi jet fighters from shooting down UAVs on their reconnaissance missions. On December 23, 2002, remote pilots of one of the Stinger-armed Predators observed an Iraqi MiG-25 turning in to attack. The Predator fired the Stinger at the MiG-25 just moments after the Iraqi aircraft launched its missile. Recorded footage showed the two missiles passing each other in the air. The Predator's missile missed, but the Iraqi missile did not.

Reportedly, this episode convinced the Iraqi Air Force that it was better for their aircraft to avoid approaching American UAVs. However, it also demonstrated to the USAF senior leadership that engaging in conflicts with vastly more agile and capable manned jet fighters did not make much sense. The experiment with Stingers was not repeated, and today it is only mentioned as an interesting footnote in the rich history of large unmanned aircraft.[91]

In discussing the interaction between UAVs and manned aircraft, we could also mention research aimed at fostering cooperation between these two types of aircraft against adversarial targets, whether manned or unmanned.[92] This brings into focus the concept of manned-unmanned teaming (MUM-T). General Dynamics has been working on this approach with its F-16 X-62 Vista, while in Europe, AIRBUS is engaged in the Future Combat Air System (FCAS) project.

5. Ground drones – battling complex environments

As demonstrated in the previous chapters, UAVs have come a long way and have reached a high level of applicability. After years of refinement, they are now widely used in various forms and sizes. On one end of the spectrum, there are UAVs such as the Black Hornet Nano, an ultra-light micro drone (only 18 g including the battery) that is small enough to fit in one hand, used by reconnaissance platoons to achieve full local situational awareness. On the other end of the spectrum are the largest Class III drones, such as the previously mentioned MQ-1 Predator, MQ-9 Reaper or the largest among them RQ-4 Global Hawk, a high-altitude long-endurance (HALE) unmanned aircraft with a gross weight of 14,600 kg. The Global Hawk is a strategic reconnaissance UAV capable of being used in missions requiring exceptional endurance (34+ hours) and an outstanding service ceiling of 18,000 m.

Aerial unmanned systems operate freely over vast empty skies, especially in conditions of uncontested airspace, as was the case in Afghanistan. However, ground-based unmanned systems struggled to navigate through terrains filled with numerous

91 Boyne, 2009, pp. 42–45.
92 Maier and Schulte, 2022, pp. 4–5.

static and dynamic obstacles, resulting in their application being significantly more limited and development being challenging and considerably slower.

Announcements of armed and intelligent autonomous unmanned ground vehicles have long been a subject of debate among sociologists and war theorists who fear the emergence of so-called "killer robots". However, from an engineering perspective, these fears are currently unfounded, and killer robots still belong to the realm of science fiction. The battlefield missions, environments, and systems pose profound complexity to robot development – so profound that today's unmanned ground vehicles (UGVs) are still confined to completing predetermined tasks (such as path following) and, if possible, only in the simplest of environments (for example, a flat surface of a modern constructed road).[93]

Achieving autonomous navigation for UGVs in challenging terrain, while avoiding obstacles, has proved to be an exceptionally complex task. The Defense Advanced Research Projects Agency (DARPA) conducted a series of competitions, known as the DARPA Urban Challenge, at the beginning of the 21st century. The first two "Grand Challenges" were intended to demonstrate that autonomous ground vehicles could cover significant distances in off-road terrain, while the 2007 competition was designed to foster innovation in autonomous vehicle operation in busy urban environments. The competitions clearly highlighted the challenges that await autonomous UGVs, and despite the allure of prestige and substantial cash prizes only six teams reached the goal. Competition was fierce, with teams from almost all top U.S. tech universities participating.

Winner of the competition, Carnegie Mellon University, emphasised the complexity of modelling the moving robot environment and the challenges of avoiding both static and dynamic obstacles. The motion planning subsystem consisted of two planners, each capable of avoiding static and dynamic obstacles while approaching a desired goal.[94] Interestingly, even in the final round, collisions occurred when multiple vehicles found themselves on the same streets of the simulated town – and this happened despite vehicles being equipped with an array of sensors (2D lidar, 3D lidar, camera, GPS positioning, Doppler radar, a stationary beam LIDAR sensor, laser scanner, etc.).

Regarding autonomy (which remains a challenging aspect for ground robots), there are three degrees of machine autonomy:

1. **Pre-programmed Autonomy**: This refers to the machine's ability to carry out a specific set of actions by following instructions pre-programmed by an operator. In the context of weaponry, an example could be the Phalanx automated gun-based close-in weapon system. Once activated, it can autonomously select and engage targets within the narrow parameters of its programming.
2. **Supervised Autonomy**: This means that a robot is capable of autonomously performing most of its functions without relying exclusively on

93 Monckton, 2018, p. 30.
94 Urmson et al., 2009, p. 3.

pre-programmed behaviours. However, in more complex or sensitive functions such as weapons release, it is still controlled by a human pilot.
3. **Complete Autonomy**: This indicates that a robot can perform all actions completely autonomously without the need for any human input. Such robots must possess a certain level of AI, allowing them to learn independently and modify their behaviour accordingly.[95]

Interestingly, more than two decades ago, several authors realistically estimated that robots were not yet intelligent enough. However, they believed that AI could reach a sufficient level to take over autonomous robot control by 2030.[96] Now, in the year when the development of AI has astonished the world, it seems that the early-century estimate was entirely realistic. But it is still unknown when AI will reach a sufficiently high level to create a turning point in the development of autonomous ground robots and UGVs.

5.1. Advantages of Robots

It seems certain that robots will take over more and more tasks from human soldiers. Increased autonomy, especially, will lead to such an outcome. The development of such systems is facilitated by the decreasing costs of technology (due to mass production and miniaturisation), greater speed in sensing, measuring, and analysing large sets of data, the resilience of robots and their ability to function under extreme weather conditions where human beings could not, and their greater resistance to wear and tear during conflicts that cause physical fatigue in humans. Furthermore, there are numerous cultural and moral advantages to robots that have no problems eliminating an opponent, do not develop PTSD, and avoid the currently dominant respect for human life as the highest value.[97]

In the realm of politics and decision-makers who determine engagement in armed conflicts, robots offer the advantage of being an easier sacrifice than a human soldier, consequently alleviating the pressure placed on leaders by the public and voters. Compared to people, machines are more resilient and stronger: they do not get tired, but can handle monotonous processes. In other words, robots cope better with the so-called 'dull, dirty, and dangerous jobs',[98] which include extended reconnaissance missions that stretch the limits of human endurance to its breaking point, environmental sampling after a nuclear or biochemical attack, and finally neutralising improvised explosive devices (IEDs).

95 Krishnan, 2009, pp. 43–45.
96 Ichbiah, 2005, p. 507.
97 Szegedi et al., 2017, p. 222.
98 U.S. Department of Defense, 2005, pp. 1–2.

5.2. Counter-IED Efforts: Where Robots are Indispensable

Unfortunately, for the last couple of decades, the headlines have been dominated by victims of IED and the dreadful casualties they cause. ReliefWeb, a humanitarian information service run by the United Nations Office for the Coordination of Humanitarian Affairs, states on its website:

> Over the last decade – between October 2010 and the end of September 2020, there have been 28,729 incidents of explosive violence, resulting in 357,619 casualties (263,487 civilians) recorded in English language media worldwide. Of these, 171,732 people were recorded as being from IEDs – a number that includes both civilians and armed actors. 48% of all people killed or injured by explosive weapons globally, then, were harmed by IEDs.[99]

Other sources state that IEDs have caused approximately half of U.S. and UK troop casualties in Iraq since 2003. Media more open to sharing information than official sources report that by 2007, the U.S. had deployed over 5,000 robots in Iraq and Afghanistan, which neutralised 10,000 IEDs – and the number of both robots and IEDs kept growing in the following years.

These robots have saved numerous lives, both of soldiers and civilians. They are remotely operated and equipped with cameras and communication devices, with their manipulator or arm being particularly suitable for inspecting potential bombs and placing explosives on them for neutralisation. Among the most iconic are the PackBot series, military robots developed and produced by Endeavor Robotics, an international robotics company founded in 2016 with roots and extensive experience dating back to iRobot (which had been producing military robots since 1990). The current base model is PackBot 510, controlled using a videogame-style hand controller. There are various versions of the 510 family, some featuring an explosive ordnance disposal (EOD) kit, a fast tactical manoeuvring kit designed for infantry troops, or a HazMat Detection Kit that collects air samples to detect chemical and radiological agents, among others.

Thanks to extensive testing and subsequent use on real battlefields, the PackBot has proven its reliability and wide applicability. Attempts have been ongoing for years to assign new roles to it. Four such projects were presented in the *Proceedings* journal: CHARS, a chemical and radiation sensor payload deployed on PackBots to search for chemical and nuclear weapons in Iraq; Griffon, a man-portable hybrid UGV/UAV based on the PackBot with a gasoline engine and a parafoil wing; Valkyrie, a man-portable battlefield casualty extraction robot based on the PackBot, and finally, Wayfarer, a project aimed at developing autonomous urban navigation capabilities for PackBots and other UGVs.[100]

99 Overton, 2020.
100 Yamauchi, 2004, pp. 230–232.

Of particular interest is the last project, which aims to enable the PackBot to perform urban reconnaissance tasks autonomously. If successful, the robot could be assigned tasks such as reconnaissance along a specified route or street, or surveillance of a specific perimeter. To achieve this, it is equipped to detect and avoid obstacles in an environment with a complex 3D structure, where the UGV may be tilted to any orientation and not only parallel to the ground plane. The Wayfarer project is just one of the many projects aiming to achieve completely autonomous robots for urban or field conditions. A lot of them are underway even today, but for now, everything still remains at the prototype level.

5.3. Large U.S. Army Robots

We will illustrate the development of UGVs using the example of the U.S. Army, which uses two major types of autonomous and semi-autonomous unmanned ground vehicles:

1. Large vehicles, such as tanks, trucks and HUMVEEs;
2. Small vehicles, which may be carried by a soldier in a backpack, such as the PackBot described earlier.

DARPA has developed, in cooperation with Carnegie Mellon University, a 6-tonne unmanned vehicle known as the Crusher, capable of carrying 1000 kg at about 50 km/h and capable of withstanding a mine explosion; it can be equipped with one or more guns. There are no intentions to deploy the Crusher vehicle in active service – instead, it will serve as the base for the development of future unmanned vehicle designs.[101]

Recent reports indicate that engineers at the U.S. Army Combat Capabilities Development Command Aviation & Missile Center are testing the Autonomous Multi-Domain Launcher (AML). This resilient autonomous UGV is based on the HIMARS but has been enhanced with both hardware and software modifications to enable remote control or autonomous operation. Weighing 17 tonnes and featuring six wheels, this vehicle is designed to navigate through open country, traversing terrains without paved roads but featuring cliffs, holes, and hidden obstacles. AML offers a wingman concept to soldiers already on the battlefield. Serving as a supplementary missile launcher, it amplifies the capabilities of the HIMARS system, which requires reloading once all six rounds are fired. However, with an AML alongside, equipped with an additional 12 missiles, the firepower and ability to support frontline troops are significantly multiplied.[102] In 2021, the Army shared a video depicting C-130s landing on an island, where they unloaded a manned HIMARS and an unmanned AML. The two operated collaboratively as a manned-unmanned team, engaging enemy threats and subsequently returning to the C-130s, which swiftly departed.

101 Lin et al., 2008, p. 13.
102 Davis Skelley, 2022.

The video showed the launcher firing Precision Strike Missiles (PrSM), highlighting one of the Army's new long-range firepower capabilities.[103]

Still, as remarkable as large vehicles may be, it is currently the small vehicles that are having their moment of glory. These small robots are the ones that approach suspicious packages left at airports, assisted in search and rescue efforts at Ground Zero after 9/11, and played a crucial role in clean-up operations following the Fukushima meltdown. They have also disarmed countless IEDs in Iraq and Afghanistan – and earned a place in the popular culture of today.

5.4. Armed Robots and Their Use in Combat

Russian sources reported[104] (and Western sources echoed[105]) that the first use of robots in combat occurred at the end of December 2015 in Latakia, a province of Syria. Six Platform-M robotic systems and four Argo systems participated in the operation, with robot attacks supported by self-propelled artillery Akatsiya systems and Syrian soldiers. Reconnaissance was conducted using UAVs. Gathering intelligence, robot control, and target designation for self-propelled cannons were coordinated from the 5 km distant command vehicle of the latest automated troop management system, Andromeda-D, which replaced Polet-K. During the alleged attack, robots were the first to engage: they approached within 100 metres of Syrian rebels and opened fire. The rebels responded, thus revealing their firing positions. Subsequently, they were targeted by self-propelled cannons coordinated by Andromeda-D. After a brief 20-minute battle, the rebels fled, leaving their dead and wounded behind. According to Russian sources, 70 rebels were killed on that occasion, while only four soldiers were reportedly injured. While the accuracy of this account remains somewhat uncertain, it certainly suggests a possible direction for future research and the goals that military planners may hope to achieve.

Platform-M is a robotic system based on a self-propelled armoured tracked chassis. It is remotely operated, equipped with a machine gun, grenade launcher, and anti-tank missile launcher, along with various sensors – a radar, thermal camera, rangefinder, video camera, and CBRN analyser. It weighs 800 kg and has a payload capacity of 300 kg. Its speed is not particularly impressive (12 km/h), but it boasts decent autonomy (10 hours). The pilot can control it visually at a distance of up to 1500 m, and the range significantly increases if video cameras or communication through a companion UAV are used.

The Argo robot on a wheeled chassis is even more impressive. It weighs a tonne, and is armed with a machine gun and four grenade launchers. Its maximum land speed is 20 km/h, and in water, it can reach 4.6 km/h. Its autonomy is an impressive

103 Eversden, 2022.
104 Tuchkov, 2016.
105 Urcosta, 2018.

20 hours. As for the U.S.-originated armed robot vehicles, the following two could be mentioned:

(1) the Talon SWORDS (Special Weapons Observation Reconnaissance Detection System) made by Foster-Miller, which can be equipped with machine guns, grenade launchers, or anti-tank rocket launchers as well as cameras and other sensors; and

(2) the MAARS (Modular Advanced Armed Robotic System). While vehicles like SWORDS and the newer MAARS can autonomously navigate towards specific targets using their GPS, complex tasks such as firing onboard weapons are conducted by a soldier located at a safe distance. Foster-Miller provides a universal control module for the war fighter to use with any of their robots. The MAARS features a more powerful machine gun than the original SWORDS. While the original SWORDS weighed about 70 kg, MAARS weighs around 160 kg. It is equipped with a new manipulator capable of lifting 45 kg, allowing it to replace its weapon platform with an IED identification and neutralisation unit.[106]

Talon robots have demonstrated their value as a counter-IED tool. In 2000, during the U.S. military intervention in Bosnia, the first Talon robots were deployed to assist in the removal of enemy explosives. Subsequently, hundreds of Talon EOD robots have been deployed in Iraq and Afghanistan. They are used in military missions as armed robots capable of maintaining a designated perimeter or deterring enemy attacks, but there have been some contradictory reports on their effectiveness,[107] and it seems that they have been grounded before seeing any real action. The first armed ground robots deployed onto a battlefield are positioned behind sandbags instead of being sent on patrol along Iraqi streets, as envisioned by their inventors. Senior Army leadership was not comfortable sending them out for combat missions due to safety reasons. The reasons should certainly be sought for the technical issues the robots faced during the testing phase. As much as these problems might have been caused by extremely unfavourable conditions of use, there was still a fear that unexpected robot behaviour could occur; therefore, they are now placed in fixed positions.[108]

The capabilities of a robot are crucial when assessing its utility in the field, but along with capabilities, reliability is equally important, especially for an armed robot. Before the Talon SWORDS robot was deployed in Iraq, there were three concerning incidents of uncommanded movements. Allegedly, all three occurred before the 2006 safety certification. A spokesperson from Foster-Miller explains how they occurred: 'One case involved a loose wire. So, now there is redundant wiring on every circuit. One involved a solder, a connection that broke. Everything now is double-soldered'. The third case was a test where the robot was placed on a 45-degree hill and left to run for two and a half hours. 'When the motor started to overheat, the robot shut the motor off, causing the robot to slide back down the incline'.[109] But

106 Lin et al., 2008, p. 12.
107 Army Technology, 2020.
108 Weinberger, 2008.
109 Ibid.

however convincing these explanations may be, they were evidently insufficient to reassure the Army's leadership (after all, we are talking about armed robots!), and therefore, these robots were put on hold.

There is a good probability that the great success of robots claimed by the Russians has also been exaggerated for propaganda purposes. This is evident from the fact that very little has been written for years about armed robots or UGVs, while UAVs have flourished and become one of the most important weapons on the modern battlefield. They have even been called the decisive factor for Azerbaijan's success in Nagorno-Karabakh[110] or 'the saviour and future of warfare' in the early months of the war in Ukraine.[111] During the same period, armed UGVs received almost no attention, a silence that speaks for itself.

5.5. What Comes Next For UGVs?

It appears that, for various reasons, armed UGVs, especially those with fully autonomous systems, will not be deployed on battlefields for some time. As previously mentioned, the use of autonomous armed robots evoked scepticism from military leaders, even when they were confronted with a technologically inferior adversary during asymmetric warfare in Iraq and Afghanistan. Consequently, the swift deployment of these robots to the battlefield seems improbable, especially considering the technological parity or superiority of potential opponents.

Nevertheless, this does not negate the current use of UGVs nor the potential plans for their future deployment. If the future development direction of UGVs cannot be determined with certainty, some of the main trends can already be anticipated. A notable example is the Ratel S (Honey Badger) UGV, proudly unveiled by the Ukrainians at the end of 2023.[112] This small, unmanned vehicle is capable of carrying grenades or even anti-tank mines. Due to its compact dimensions, it can be manoeuvred under enemy armoured vehicles and its explosive payload detonated there, targeting the most vulnerable parts of armoured vehicles and tanks where the armour is significantly thinner than on the front.

Equally important is the enhanced antenna and communication system reported for Ratel S, indicating improved counter-electronic warfare (C-EW) capabilities. This could be a crucial feature for the overall usability of the small UGV, especially when considering the formidable Russian EW systems. Russian Krakushas and Leers boast a high success rate in halting enemy guided projectiles and unmanned vehicles, both ground and aerial.

Even at first glance, the Ratel S exemplifies the desirable traits of future UGVs – compact size and low cost of production. In contrast, large drones have proven impractical and often unsuccessful against Russian EW systems (for example, the

110 Sapmaz, 2021, pp. 11–17.
111 Shoaib, 2023.
112 Struck and Brown, 2023.

Bayraktar UAV[113]), prompting a shift towards deploying a multitude of inexpensive UAVs or UGVs, some of which have the chance to break through and strike the target. Therefore, whether the solution lies in small, expendable robots relying on numbers or in large systems with powerful counter-EW measures will be revealed in the future.

Another future development idea is marsupial robots, which are UAVs carrying smaller UAVs or UGVs within them.[114] The concept of marsupial robots offers significant possibilities, merging the mobility of UAVs with the stealthy approach capability of UGVs and effectively combining the strengths of both unmanned vehicle families. The potential applications are diverse; for instance, fast fixed-wing UAVs could serve as a mother ship, releasing a swarm of smaller rotary-wing UAVs close to the target and allowing them to infiltrate enemy bunkers and facilities.

A third idea involves reversing the scenario by establishing a connection between tele-operated UGVs and tethered UAVs. Tele-operated UGVs suffer from insufficient situational awareness due to onboard sensing limitations, but this could be rectified by a tethered UAV providing a better view of the terrain.[115] This flying visual assistant could be tele-operated, requiring an additional human operator and a coordinated crew.[116] On the other hand, possibilities expand if the UAV operates autonomously, navigating through the area where the UGV is passing.

While these concepts are presently confined to the future, it does not appear that their realisation is too far off (akin to the thought of armed robots). However, today's robots are yet to reach that level and are mainly employed for transporting cargo and offering logistical assistance to soldiers.

6. European Armies and U.S. Industries in the ERA of UAVs

An assessment of European armies reveals a notable lag in the development of UAVs over the past decades, particularly in recent years. This holds true for European manufacturers as well. According to a 2019 study,[117] competitiveness is satisfactory only in the small UAVs category but worsens for larger UAVs categories.

Utilisation of tactical UAVs is poor, and an even worse situation is in the MALE category. Virtually no HALE (High-Altitude Long Endurance) UAV exists in European armies. The study only highlights the "future procurement of Triton by Germany and the United Kingdom", referring to the potential acquisition of several

113 Clark, 2022.
114 De Petris et al., 2022, pp. 1–7.
115 Monckton, 2018, pp. 40–41.
116 Xiao et al., 2021, pp. 15–29.
117 Kunertova, 2019, pp. 10–13.

U.S. Navy MQ-4C Triton Global Hawk UAVs after abandoning the customised EuroHawk version. In the MALE and HALE category, a strong monopoly of American platforms is evident.

The same study notes that armed UAVs are virtually unused by any European military. The UK is the only European country operating the armed version of the Reaper. Other European armies, in the face of public pressure, remain reluctant to arm their UAVs, utilising them exclusively for ISR purposes. Incidentally, a similar lack of unity is evident in the legislative sphere, where for years there has been a futile attempt to adopt a uniform legal practice that would be accepted by all EU member states, as explained in Chapter 13. However, experiences from the Russo-Ukrainian War suggest that such a mindset may be out dated.

6.1. The War in Ukraine as a Wake-Up Call

The poor equipment and lack of readiness in defence sectors are a consequence of a false sense of security that has prevailed in Europe since the dissolution of the Soviet Union in the early 1990s. Since then, European armies have been continuously reduced, along with investments in the defence system, and research and development have been especially minimized. The consequences of such policies are evident today, as European states struggle to even initiate production of simple products such as 155 mm shells in long-abandoned defence industry facilities. However, the Russo-Ukrainian War has been a harsh wake-up call. Suddenly, all the problems that had been suppressed and swept under the rug for years came to the surface. One article states:

> European nations have adopted a piecemeal approach to defence – European armies have 17 types of main battle tanks and 20 different fighter aircraft, while the U.S. has one tank and six types of fighters. Europe depends on the U.S. for command and control, intelligence and surveillance, air transport, and aerial refuelling.[118]

But following Russia's brutal aggression towards Ukraine, the situation started to change: Europe's military spending has increased from USD $420.7 billion in 2021 to $480.3 billion in 2022. This represents a significant increase of 14.2%, and the growth continues in 2023. However, two urgent questions arise:

1. Should more investments be allocated to compensate for thirty years of neglecting defence systems?
2. Should independent investment in development and equipment continue, or would it be more beneficial to undertake joint projects?

118 Duncan, 2023.

6.2. Joint European UAV Programmes: Underfunded, Suboptimally Specified, Finally Abandoned

For years neglected, the development of European UAVs now needs to be accelerated to at least reduce the gap with leading players. In a recent interview,[119] Lt. Gen. Ingo Gerhartz, Chief of the German Air Force, stated that faster progress in the fielding of new military drones is needed. He specifically refers to the trinational program FCAS, involving Germany, France, and Spain. The programme promises amazing new capabilities and encompasses the development of remote carrier vehicles (swarming drones) as well as a new sixth generation jet fighter. However, the timeline has been set extremely unambitiously, and the system is only predicted to be fully operational in 2040 at the earliest. This is just one example of European projects whose development spans years and even decades, and when the first prototype finally sees the light of day, it turns out to be already outdated.

There is a long line of European programmes that have been halted due to funding issues or poor results of the initial versions.[120] For example, there was a project known as Advanced UAV or Talarion, launched in 2006 by the French, German, and Spanish governments. The Talarion UAV was built by the European Aeronautic Defence and Space Company (EADS), formed through the merger of the French Aérospatiale and the German DASA. EADS initially planned to produce 15 systems under a European programme worth around €3 billion ($3.9 billion). However, after even France, Germany, and Spain did not commit to buying the Talarion and thus provide financial backing, EADS halted future development of the UAV. In a last attempt to save the project, EADS offered the Talarion to the UK Royal Air Force, rebranding it as the "X-UAS", but the UK instead backed the Telemos UAV, a programme started in a French-British partnership.

Telemos was jointly developed by BAE Systems and Dassault. There was even an exclusive agreement between BAE Systems and Dassault not to cooperate with other partners on the development of similar UAVs, thereby reducing the risk of competition. However, even this did not results in orders being placed for Telemos by the armed forces of the two partner nations, leading to the programme being eventually discontinued in July 2012. These repeated failures ultimately encouraged European countries to acquire foreign MALE drones – and as could be expected, Europe chose the American Predator and Reaper, with the exception of Germany, which leased the Israeli Heron.

Despite recent increases, only 18% of equipment procurement within the EU was conducted jointly in 2021, a figure that falls significantly short of the 35% objective agreed upon by member states. Joint procurement is expected to enable member states to achieve economies of scale, curtail the inflation of equipment prices, and prevent smaller states from being disadvantaged or receiving services last. In order

119 Sprenger, 2023.
120 Buzzoni et al., 2022.

to avert fragmentation, price inflation, potential supply shortages, and to offer the EDTIB (European Defence Technological and Industrial Base) the necessary attention for growth, the European Commission has introduced two incentives: EDIRPA (short term) and EDIP (long term). These initiatives are designed to consolidate European demand through the encouragement of joint acquisitions and strengthen the competitiveness of the EDTIB by augmenting the production capacity of the European defence industry.[121]

Some analysts even suggest that European joint programmes are almost certainly doomed to failure.[122] Given that participating nations have different (and sometimes mutually exclusive) operational needs, defining the system features takes a long time, and the overall project ultimately ends up being suboptimally specified. Delays in the payment of national contributions also occurs quite frequently, leading to delays in production. This, in turn, compels the involved parties, as well as other potential European buyers, to acquire systems that have already been developed by a nation more efficient in the production process – most likely the United States.

6.3. Choosing to abandon R&D and buy off the shelf

Because of numerous failed joint European projects, an analyst at *The Telegraph* suggests that 'time is too short for Britain to start building its own weapons',[123] and then emphasises:

> …all across Europe and the UK, arms companies are salivating at the idea that their governments will sink huge sums into developing, from scratch, various weapons technologies that only America has… But we need this equipment quickly, and we need it to actually work and be affordable. We must stop using our defence budgets as job creation schemes and instead buy working kit off the shelf.

The author also praises Poland for opting for ready-made solutions from South Korea, Turkey, and the United States. Faced with a war on its eastern border, Poland has signed a contract with South Korean manufacturers expressing readiness to purchase weapons worth $22 billion. As part of the procurement, Poland will acquire 1000 K2 tanks, 672 self-propelled K9 howitzers (including versions produced in Poland), 288 units of the rocket artillery system MLR K239, and 48 FA-50 light combat aircraft. Poland also ordered four Bayraktar TB2 UAVs – the first in the EU to do so – and concluded a lease agreement with General Atomics to lease MQ-9A Reapers in preparation for eventual purchase.

The lessons learned from the Russo-Ukrainian War indeed underscore that when a country is on the brink of war, time emerges as a pivotal factor in safeguarding

121 Schnitzler, 2023, pp. 3–5.
122 Tilenni, 2023.
123 Page, 2023.

national security. Buying already proven solutions turns out to be more justifiable than investing in the long and uncertain R&D process for new weaponry. However, to maintain at least some of the domestic industrial capabilities could be of utmost importance later in the course of war, when new weapons (for example, small or micro UAVs) could be developed based on the existing platforms.

This is evident in Ukraine, where, faced with an ever-escalating demand, the Ukrainians modified inexpensive Chinese drones, while the Russians tailored cost-effective Iranian loitering munitions. Both sides have devised ingenious solutions to bypass EW measures installed by the other side. Mobilising their domestic industrial potential allows both sides to swiftly replenish the thousands of UAVs destroyed month after month. Such an achievement would not be feasible if this industry and corresponding know-how had been neglected and lost in the years preceding the war.

6.4. Eurodrone: Is it a MALE UAV That Nobody Needs?

Eurodrone stands as one of the most ambitious joint European projects in recent decades, aiming to provide Europe with its own MALE UAV while circumventing the strict limitations of the United States regulatory regime International Traffic in Arms Regulations.[124] Four European countries have previous experience with MALE systems: Italy uses the General Atomics MQ-9 Reaper and the MQ-1 Predator, deployed in the Middle East; France also had Reapers, while Spain have recently ordered them, and Germany has experience with the leased Israel Aerospace Industries Heron TP for reconnaissance missions in Afghanistan.[125]

However, the programme started exceptionally slowly, requiring two years to study required capabilities and an additional two years for contractor selection. The prime contractor was the German Airbus Defence and Space GmbH, with major subcontractors Airbus Defence and Space S.A.U, Leonardo, and Dassault Aviation. The construction contract was signed only in 2022, and it was agreed that 20 systems would be produced (seven for Germany, five for Italy, and four each for France and Spain). Each system comprises three flight units and two ground control stations.

Despite a prototype expected by early 2023, delays have already occurred (and are projected to continue by at least two years) due to fundamental differences in expectations among the four countries. Germany, in particular, complicated the project by insisting on Eurodrone having two engines to safely traverse its national territory. The new UAV is anticipated to weigh up to 11 tonnes, significantly more than the 4.5-tonne MQ-9 Reaper.[126]

124 This regime mandates that buyers of U.S. Predators and Reapers seek U.S. Congress permission for practically any significant use.
125 Tilenni, 2023.
126 Pons, 2022.

The main concern, however, lies in the overall cost-effectiveness of the Eurodrone. While American Predators and Reapers performed well in missions in the uncontested airspace of Afghanistan and Iraq, experiences in the Syrian war and the downing of a Reaper by Russian fighters over the Black Sea demonstrated the vulnerability of large UAVs to enemy air defences. Recent events in the war in Ukraine also indicate that large UAVs are susceptible to electronic jamming. With the delivery postponed to 2029, there is a possibility that the ambitious €7.1 billion project may become outdated by the time it is ready for use. However, tactical UAVs are becoming more cost-effective and powerful, offering the best current combination of cost and capabilities.[127]

6.5. Tactical UAVs: The Most Promising UAV Class of Today

The conflict in Ukraine has showcased the extensive capabilities of small and medium-range tactical UAVs. These aircraft, which come at a relatively low cost, effectively carry out intelligence gathering, surveillance, target acquisition, and reconnaissance (ISTAR). While they may be less autonomous to MALE drones, tactical UAVs prove equally valuable at the operational level. Under favourable conditions, they have even been deployed for attack missions targeting enemy personnel, equipment, vehicles, and structures. Moreover, they offer significant propaganda potential by leveraging footage captured through onboard cameras. Current experiments explore the integration of EW equipment onto these platforms.

Recognising their value, all EU countries with advanced armed forces understand the potential of incorporating tactical UAVs in their strategic plans. But despite shared operational requirements, most nations have opted for independent solutions, driven by political and industrial considerations to support their respective national defence industries. The consequence is the foreseeable proliferation of individual programmes.

This lack of collaboration leads to duplicated efforts and increased costs, especially given that nearly all countries stipulate similar requirements for their tactical UAVs. Notable examples include French Safran's development of the Patroller UAV, Spain's joint project with Colombia on the Sistema Remotamente Tripulado de Altas Prestaciones (SIRTAP) tactical UAV, and Italy's initiative with the Leonardo FALCO EVO. Each of these tactical UAVs boasts an endurance of over 20 hours, a range of approximately 200 km, a payload of around 200 kg, a ceiling of 6000 m, and a maximum speed of around 200 km/h. The associated costs are considerable – around EUR 500 million per country.[128] Many other European countries have developed tactical UAVs, independently, such as Germany (Rheinmetall LUNA NG), Greece (HAI Pegasus), Hungary (ProTAR), and others.

127 Kunertova, 2022, pp. 3–4.
128 Tilenni, 2023.

Given their favourable cost-effectiveness, tactical UAVs are likely to become more prevalent in the armed forces of Europe and beyond. Rather than emphasising competition or exclusivity between tactical and MALE UAVs, it would make more sense to view one class as complementing the other. As suggested in a 2022 analysis, European countries should 'adopt a holistic approach on drones and anti-drone defences.'[129] This approach involves drawing pertinent lessons from the conflict in Ukraine, and, accordingly, fostering UAV diversity. Different UAV classes serve distinct military roles and offer varying effects. Therefore, European countries should align their drone acquisition strategies to encompass a comprehensive spectrum of UAVs – if resources allow it. If funding constraints arise, opting for a larger number of smaller UAVs appears more viable than investing in one or two large MALE UAVs. The anticipated progress in AI could further elevate weaponry capabilities, especially for smaller UAVs, bringing them to an entirely new level.

7. Conclusion

The robots and drones of today represent a true breakthrough in military technology and the way wars are fought. Enhanced with each new version, they offer astonishing capabilities in practically all aspects of military operations. However, in the rapidly changing world of modern technology, it is challenging to predict which of these systems will succeed and establish themselves as indispensable solutions and which may disappear from the battlefield or undergo a fundamental transformation.

One category with an uncertain future is large MALE and HALE UAVs. It is possible that they will become more agile and similar to today's manned aircraft in the future, or they might evolve into mere carriers of smaller UAVs that will then perform the majority of tasks.

Based on experiences from Ukraine, tactical UAVs are increasingly emerging as highly desirable and versatile solutions. Their agility and adaptability make them exceptionally useful, suggesting that they could play a significant role in future conflicts. If this happens, existing military strategies will need to be revised, and technological development may shift towards the creation of small or micro UAVs that operate in swarms to overcome enemy EW systems.

While UAVs dominate the airspace, ground robots/drones (UGVs) still struggle to find their place on the battlefield. Unlike UAVs, which are already integrated into military operations, UGVs are still in the early stages of development. Their final future depends on the development of artificial intelligence (AI) which will

129 Kunertova, 2022, p. 2.

enable them to efficiently navigate around obstacles and find optimal routes to their targets.

As things stand now, the future of warfare is likely to involve a diverse fleet of both large and small UAVs. Managed by AI systems, they will collaborate with UGVs to achieve the goals of complex military operations. Existing technologies, as well as those currently in development, will collectively shape future military strategies and contribute to a paradigm shift in the way wars are conducted.

References

Adamowski, J. (2022) 'Poland leases MQ-9A Reapers ahead of drone buy', *Defense News*, 21 October 2022. [Online]. Available at: https://www.defensenews.com/global/europe/2022/10/21/poland-leases-mq-9a-reapers-ahead-of-drone-buy/ (Accessed: 5 January 2024).

Aegerter, G. (2013) 'Drone worth millions crashes into Lake Ontario, military says', *NBC News*, 12 November 2013. [Online]. Available at: https://www.nbcnews.com/news/world/drone-worth-millions-crashes-lake-ontario-military-says-flna2d11582458 (Accessed: 5 January 2024).

Attariwala, J. (2017) 'MQ-9B SkyGuardian', *Canadian Defence Review*, 23(5), pp. 19–23.

Bartulović, V., Trzun, Z., Hoić, M. (2023) 'Use of Unmanned Aerial Vehicles in Support of Artillery Operations', *Strategos*, 7(1), pp. 71–92.

Ben-Ari, M., Mondada, F. (2018) 'Robots and Their Applications' in Ben-Ari, M., Mondada, F. (eds.) *Elements of Robotics*. New York, NY: Springer International Publishing, pp. 1–20, https://doi.org/10.1007/978-3-319-62533-1_1.

Bird, S.M., Fairweather, C.B. (2007) 'Military fatality rates (by cause) in Afghanistan and Iraq: a measure of hostilities', *International Journal of Epidemiology*, 36(4), pp. 841–846.

Blom, J. (2010) *Unmanned Aerial Systems: A Historical Perspective*. Leavenworth, WA: Combat Studies Institute Press and US Army Combined Arms Center Fort Leavenworth.

Boyne, W.J. (2009) 'How the Predator Grew Teeth', *Air And Space Forces Magazine*, 1 July 2009. [Online]. Available at: https://www.airandspaceforces.com/article/0709predator/ (Accessed: 5 January 2024).

Breen, K. (2023) 'Russian fighter jet damages U.S. drone flying over Syria, U.S. military says', *CBS News*, 25 July 2023. [Online]. Available at: https://www.cbsnews.com/news/russian-fighter-jet-damages-us-drone-flying-over-syria-video-shows-military/ (Accessed: 5 January 2024).

Buzzoni, L., Brillaud, L., Schmidt, N. (2022) 'The Eurodrone: An industrial project fuelled by politics', *Investigate Europe*, 31 March 2022. [Online]. Available at: https://www.investigate-europe.eu/posts/eurodrone (Accessed: 5 January 2024).

Chamayou, G. (2015) *A Theory of the Drone*. New York, NY: The New Press.

Clark, B. (2022) 'The Fall and Rise of Russian Electronic Warfare', *IEEE Spectrum*, 30 July 2022. [Online]. Available at: https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare (Accessed: 5 January 2024).

Cohen, R.S. (2022) 'Air Force's first Pacific MQ-9 squadron comes at crossroads for drone', *Air Force Times*, 25 October 2022. [Online]. Available at: https://www.airforcetimes.com/news/your-air-force/2022/10/25/air-forces-first-pacific-mq-9-squadron-comes-at-crossroads-for-drone/ (Accessed: 5 January 2024).

Cole, C. (2015) 'What 200 military drone crashes tells us about the drone wars', *Drone Wars UK*, 27 February 2015. [Online]. Available at: https://dronewars.net/2015/02/27/what-200-military-drone-crashes-tells-us-about-the-drone-wars/ (Accessed: 5 January 2024).

Cuadra, A., Whitlock, C. (2014) 'How drones are controlled', *The Washington Post*, 20 June 2014. [Online]. Available at: https://www.washingtonpost.com/wp-srv/special/national/drone-crashes/how-drones-work/ (Accessed: 5 January 2024).

Davis-Skelley, K. (2022) 'Testing of the Army's first autonomous vehicle speeds ahead', *DEVCOM Aviation & Missile Center Public Affairs*, 11 August 2022. [Online]. Available at: https://www.army.mil/article/259244/testing_of_the_armys_first_autonomous_vehicle_speeds_ahead (Accessed: 5 January 2024).

De Petris, P., Khattak, S., Dharmadhikari, M., Waibel, G., Nguyen, H., Montenegro, M., Khedekar, N., Alexis, K., Hutter, M. (2022) 'Marsupial Walking-and-Flying Robotic Deployment for Collaborative Exploration of Unknown Environments', *2022 IEEE International Symposium on Safety, Security, and Rescue Robotics*, pp. 188–194.

Department of Defense, Inspector General (2020) *Evaluation of Weather Support Capabilities for the MQ-9 Reaper*. Washington, DC: US Department of Defense.

Doaré, R., Danet, D., Hanon, J.-P., de Boisboissel, G. (2014) *Robots on the battlefield – Contemporary issues and implications for the future*. Leavenworth, WA: Combat Studies Institute Press US Army Combined Arms Center Fort Leavenworth.

Donald, D. (2018) 'U.S. Air Force Ends Predator Operations', *AIN Media Group*, 13 March 2018. [Online]. Available at: https://www.ainonline.com/aviation-news/defense/2018-03-13/us-air-force-ends-predator-operations (Accessed: 5 January 2024).

Duncan, M. (2023) 'Europe's defence goals', *Graphic News*, 2 May 2023. [Online]. Available at: https://www.graphicnews.com/en/pages/44231/military-europes-defence-goals (Accessed: 5 January 2024).

Evans, A., Harward, C., Grace, M., Stepanenko, K.K.F.W. (2023) 'Russian Offensive Campaign Assessment, November 25, 2023', *The Institute for the Study of War*. [Online]. Available at: https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-25-2023 (Accessed: 5 January 2024).

Eversden, A. (2022) 'Army's autonomous HIMARS moving forward, will be at Project Convergence', *Breaking Defense*, 17 June 2022. [Online]. Available at: https://breakingdefense.com/2022/06/armys-autonomous-himars-moving-forward-will-be-at-project-convergence (Accessed: 5 January 2024).

Frantzman, S.J. (2021) *The Drone Wars: Pioneers, Killing Machines, Artificial Intelligence, and the Battle for the Future*. New York, NY: Bombardier Books.

Gibb, R.W., Olson, W. (2008) 'Classification of Air Force Aviation Accidents: Mishap Trends and Prevention', *The International Journal of Aviation Psychology*, 18(4), pp. 305–325; https://doi.org/10.1080/10508410802346913.

Gittins, P. (ed.) (2020) *A Global Security System: An Alternative to War*. World Beyond War.

Goodrich, P.S. (2003) *The Surgical Precision Myth: After the Bomb Explodes – (CCDP) Cumulative Collateral Damage Probability*. Providence, RI: Providence College (unpublished manuscript).

Gosselin-Malo, E. (2023) 'Reveal of French-made combat drone stirs up industry', *C4ISR.Net*, 19 June 2023. [Online]. Available at: https://www.c4isrnet.com/global/europe/2023/06/19/reveal-of-french-made-combat-drone-stirs-up-industry/ (Accessed: 5 January 2024).

Grossman, N. (2019) 'Trump Cancels Drone Strike Casualty Report: Does It Matter?', *War On The Rocks*, 2 April 2019. [Online]. Available at: https://warontherocks.com/2019/04/trump-cancels-drone-strike-civilian-casualty-report-does-it-matter/ (Accessed: 5 January 2024).

Gundlach, J. (2012) *Designing Unmanned Aircraft Systems: A Comprehensive Approach*. Schetz, J.A. (ed.) Published online: American Institute of Aeronautics and Astronautics, Inc.

Haider, U. (2023) 'Indian Navy's Mq-9b Sea Guardian Purchase Puts Pakistan's Subs on Notice', *Geopolitical Monitor*, 26 September 2023. [Online]. Available at: https://www.geopoliticalmonitor.com/indian-navys-mq-9b-sea-guardian-purchase-puts-pakistans-subs-on-notice/ (Accessed: 5 January 2024).

Herold, M. (2008) 'Illusion: Our modern military warfare only kills the "bad guys."' in P. Buchheit, P. (ed.) *American Wars: Illusions and Realities*. Atlanta, GA: Clarity Press, pp. 97–99.

Human Rights Watch (2014) 'A Wedding That Became a Funeral: US Drone Attack on Marriage Procession in Yemen', 19 February. [Online]. Available at: https://www.hrw.org/report/2014/02/19/wedding-became-funeral/us-drone-attack-marriage-procession-yemen (Accessed: 5 January 2024).

Ichbiah, D. (2005) *Robots: From Science Fiction to Technological Revolution*. New York, NY: Harry N. Abrams publishing.

Insinna, V. (2021) 'Get ready for another fight over the future of the MQ-9 Reaper', *Defense News*, 26 May 2021. [Online]. Available at: https://www.defensenews.com/air/2021/05/26/get-ready-for-another-fight-over-the-future-of-the-mq-9-reaper/ (Accessed: 5 January 2024).

International Organization for Standardization [ISO] (2021) *ISO 8373:2021(en) Robotics – Vocabulary*. International Organization for Standardization [ISO].

Jha, A. (2017) *Theory, Design, And Applications Of Unmanned Aerial Vehicles*. Boca Raton, FL: CRC Press; https://doi.org/10.1201/9781315371191.

Khan, A. (2021) 'Hidden Pentagon Records Reveal Patterns Of Failure In Deadly Airstrikes', *New York Times*, 18 December 2021. [Online]. Available at: https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian-deaths.html (Accessed: 5 January 2024).

Kokkinidis, T. (2022) 'US Deploys Eight MQ-9 Reaper Drones to Greece', *GreekReporter*, 26 November 2022. [Online]. Available at: https://greekreporter.com/2022/11/26/us-deploys-eight-mq-9-reaper-drones-greece/ (Accessed: 5 January 2024).

Krishnan, A. (2009) *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Farnham, UK: Ashgate Publishing Limited.

Kunertova, D. (2019) *Military Drones in Europe: The European Defense Market and the Spread of Military UAV Technology*. Syddansk Universitet, Danemark: Center for War Studies.

Kunertova, D. (2022) 'The Ukraine Drone Effect on European Militaries', *Policy Perspectives*, 10(15); https://doi.org/10.3929/ethz-b-000584078.

Larson, C. (2020) 'Sparrowhawk: This Drone Can Be Launched from the Air and Recovered by a Mothership', *The National Interest*, 30 September 2020. [Online]. Available at: https://nationalinterest.org/blog/buzz/sparrowhawk-drone-can-be-launched-air-and-recovered-mothership-169856 (Accessed: 5 January 2024).

Liebermann, O. (2023) 'Russian fighter jet damages US military drone over Syria', *CNN*, 25 July 2023. [Online]. Available at: https://edition.cnn.com/2023/07/25/politics/russia-us-drone-damaged-syria/index.html (Accessed: 5 January 2024).

Light, T., Hamilton, T., Pfeifer, S. (2020) *Trends in U.S. Air Force Aircraft Mishap Rates (1950-2018)*. RAND Corporation; https://doi.org/10.7249/RRA257-1.

Lin, P., Bekey, G., Abney, K. (2008) *Autonomous Military Robotics: Risk, Ethics, and Design*. San Luis Obispo, CA: California Polytechnic State University.

Magnuson, S. (2010) 'Robot Manufacturers Lament Absence of Strong Army Advocate. National Defense', *National DEFENSE*, 19 March 2010. [Online]. Available at: https://www.nationaldefensemagazine.org/articles/2010/3/19/robot-manufacturers-lament-absence-of-strong-army-advocate (Accessed: 5 January 2024).

Maier, S., Schulte, A. (2022) 'A Cloud-based approach for synchronous multi-pilot multi-UAV mission plan generation in a MUM-T environment', *AIAA SCITECH 2022 Forum*; https://doi.org/10.2514/6.2022-2345.

Martin, J. (2013) 'RPA reservists help reach 2 million-hour milestone', *Air Force Reserve Command*, 1 November 2013. [Online]. Available at: https://www.afrc.af.mil/News/Article/561434/rpa-reservists-help-reach-2-million-hour-milestone/ (Accessed: 5 January 2024).

McCarthy, N. (2020) 'The Mammoth Cost Of Operating America's Combat Aircraft', *Statista*, 26 November 2020. [Online]. Available at: https://www.statista.com/chart/23618/operating-cost-per-aircraft/ (Accessed: 5 January 2024).

McClure, M. (2015) '5 big problems with the drone programs', *Foreign Policy*, 10 December 2015. [Online]. Available at: https://foreignpolicy.com/2015/12/10/5-big-problems-with-the-drone-programs/ (Accessed: 5 January 2024).

McDermott, R. (2017) *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. Tallinn: International Centre for Defence and Security.

Michel, A.H. (2013) 'Drones in Bosnia', *Drone Center*, 7 June 2013. [Online]. Available at: https://dronecenter.bard.edu/drones-in-bosnia/ (Accessed: 5 January 2024).

Milburn, A. (2021) 'Drone Strikes Gone Wrong: Fixing a Strategic Problem', *Small Wars Journal*, 10 August 2021. [Online]. Available at: https://smallwarsjournal.com/jrnl/art/drone-strikes-gone-wrong-fixing-strategic-problem (Accessed: 5 January 2024).

Monckton, S. (2018) 'Current And Emerging Technology In Military Robotics.' in Braun, W.G., von Hlatky, S., Nossal, K.R. (eds.) *Robotics And Military Operations*. Carlisle, PA: The Strategic Studies Institute and U.S. Army War College Press.

Mulrine, A. (2008) 'Warheads on Foreheads', *Air Force Magazine*, October 2008, pp. 44–47.

NATO Publication (2019) *ATP 3.3.8.1-Minimum Training Requirements for Unmanned Aircraft Systems (UAS) Operators And Pilots* (p. 58). Washington, DC: United States Department of Defense.

Olney, B. (2019) 'New system allows NY ANG MQ-9s to fly without chase planes', *Air National Guard*, 11 September 2019. [Online]. Available at: https://www.ang.af.mil/Media/Article-Display/Article/1957391/new-system-allows-ny-ang-mq-9s-to-fly-without-chase-planes/ (Accessed: 5 January 2024).

Olson, E., Chappell, B. (2023) 'The U.S. military releases footage of Black Sea drone crash with Russian jet', *NPR*, 16 March 2023. [Online]. Available at: https://www.npr.org/2023/03/16/1163845903/video-drone-crash-russia-black-sea (Accessed: 5 January 2024).

Overton, I. (2020) 'A decade of global IED harm reviewed', *ReliefWeb and Action on Armed Violence*, 15 October 2020. [Online]. Available at: https://reliefweb.int/report/world/decade-global-ied-harm-reviewed (Accessed: 5 January 2024).

Page, L. (2023) 'Time is too short for Britain to start building its own weapons', *The Telegraph*, 9 December 2023. [Online]. Available at: https://www.telegraph.co.uk/business/2023/12/09/putin-russia-war-economy-an-existential-threat-to-europe/ (Accessed: 5 January 2024).

Palik, M., Nagy, M. (2019) 'Brief History of UAV Development', *Repüléstudományi Közlemények*, 31(1), pp. 155–166; https://doi.org/10.32560/rk.2019.1.13.

Pons, J. (2022) 'Spain partners with Germany, France and Italy to build Europe's largest military drone', *Atalayar: Between Two Shores*, 30 January 2022. [Online]. Available at: https://www.atalayar.com/en/articulo/new-technologies-innovation/spain-partners-germany-france-and-italy-build-europes-largest-military-drone/20220129110021154853.html (Accessed: 5 January 2024).

Ranquist, E., Steiner, M., Argrow, B. (2017) *Exploring the range of weather impacts on UAS operations*. 18th Conference on Aviation, Range and Aerospace Meteorology. 22–26 January 2017. Seattle, WA: American Meteorological Society (AMS).

Roza, D. (2023) 'AFSOC Wants MQ-9 Reapers to Act As 'Capital Ships' For Smaller Drones', *Air And Space Forces Magazine*, 19 September 2023. [Online]. Available at: https://www.airandspaceforces.com/mq-9-reapers-afsoc-smaller-drones/ (Accessed: 5 January 2024).

Sapmaz, A. (2021) *The Role Of Unmanned Aerial Vehicle, Armed Unmanned Aerial Vehicle And Drones In The Second Karabakh War*. 3. International Baku Scientific Research Congress. Baku, October 15-16, 2021: Baku Eurasia University.

Savage, C., Schmitt, E., Khan, A., Hill, E., Koettl, C. (2022) 'New Footage Shows the Risk Of Drone War', *New York Times*, 20 January 2022. [Online]. Available at: https://www.nytimes.com/2022/01/19/us/politics/afghanistan-drone-strike-video.html (Accessed: 5 January 2024).

Schmitt, E. (2021) 'No Penalty Over U.S. Strike That Killed Civilians', *New York Times*, 14 December 2021. [Online]. Available at: https://www.nytimes.com/2022/01/19/us/politics/afghanistan-drone-strike-video.html (Accessed: 5 January 2024).

Schmitt, E., Cooper, H. (2021) 'Drone Attack Was a Mistake, Pentagon Says', *New York Times*, 18 September 2021. [Online]. Available at: https://www.nytimes.com/2021/09/17/us/politics/pentagon-drone-strike-afghanistan.html (Accessed: 5 January 2024).

Schmitt, E., Cooper, H. (2023) 'Attack on U.S. Drone by Russian Jets Is Seen in 42-Second Pentagon Video', *New York Times*, 17 March 2023. [Online]. Available at: https://www.nytimes.com/2023/03/16/us/politics/russia-drone-black-sea.html (Accessed: 5 January 2024).

Schnitzler, G. (2023) *EDIRPA/EDIP: Risks And Opportunities Of Future Joint Procurement Incentives For The European Defence Market*. Paris: The French Institute for International and Strategic Affairs (IRIS).

Shoaib, A. (2023) 'Bayraktar TB2 drones were hailed as Ukraine's savior and the future of warfare. A year later, they've practically disappeared', *Business Insider*, 28 May 2023. [Online]. Available at: https://www.businessinsider.com/turkeys-bayraktar-tb2-drones-ineffective-ukraine-war-2023-5 (Accessed: 5 January 2024).

Shoker, S. (2021) *Military-Age Males in Counterinsurgency and Drone Warfare*. New York, NY: Palgrave Macmillan Cham; https://doi.org/10.1007/978-3-030-52474-6.

Singer, P. (2009) *Wired for War: the Robotics Revolution And Conflict in the Twenty-first Century*. London: The Penguin Press.

Sloggett, D. (2015) *Drone Warfare: The Development of Unmanned Aerial Conflict*. New York, NY: Skyhorse.

Smith, M. (2016) '2015 Marked the Worst Year for Drone Crashes the Air Force Has Ever Had', *Industry Tap*, 26 January 2016. [Online]. Available at: https://www.industrytap.com/2015-marked-worst-year-drone-crashes-air-force-ever/34095 (Accessed: 5 January 2024).

Smith, P. (2020) *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy*. American Security Project.

Sprenger, S. (2023) 'German air chief urges haste in fielding strike, utility drones', *Defense News*, 3 November 2023. [Online]. Available at: https://www.defensenews.com/global/europe/2023/11/03/german-air-chief-urges-haste-in-fielding-strike-utility-drones/ (Accessed: 5 January 2024).

Stashevskyi, O., Bajak, F. (2022) 'Deadly secret: Electronic warfare shapes Russia-Ukraine war', *Associated Press*, 4 June 2022. [Online]. Available at: https://apnews.com/article/russia-ukraine-kyiv-technology-90d760f01105b9aaf1886427dbfba917 (Accessed: 5 January 2024).

Stevenson, B. (2015) 'MoD reveals Reaper derivative will be chosen for Protector', *Flight Global*, 7 October 2015. [Online]. Available at: https://www.flightglobal.com/civil-uavs/mod-reveals-reaper-derivative-will-be-chosen-for-protector/118450.article (Accessed: 5 January 2024).

Struck, J., Brown, S. (2023) 'Ukraine Has a New Ground 'Drone' – the Ratel S (Honey Badger) UGV', *Kyiv Post*, 24 October 2023. [Online]. Available at: https://www.kyivpost.com/post/23189 (Accessed: 5 January 2024).

Szegedi, P., Koronvary, P., Békési, B. (2017) 'The Use Of Robots In Military Operations', *Scientific Research And Education In The Air Force*, 2017/19, pp. 221–230; https://doi.org/10.19062/2247-3173.2017.19.1.25.

Tilenni, G. (2023) 'UAV Programmes: a Focus on the EU', *European Security & Defence*, 3 August 2023. [Online]. Available at: https://euro-sd.com/2023/08/articles/32890/uav-programmes-a-focus-on-the-eu/ (Accessed: 5 January 2024).

Tirpak, J.A. (2021) 'Air Force to Upgrade MQ-9's Mission and Capabilities for Near-Peer Fight', *Air And Space Forces Magazine*, 21 April 2021. [Online]. Available at: https://www.airandspaceforces.com/air-force-to-upgrade-mq-9s-mission-and-capabilities-for-near-peer-fight/ (Accessed: 5 January 2024).

Tisseron, A. (2014) 'Robotic and Future Wars: When Land Forces Face Technological Developments' in Doaré, R., Danet, D., Hanon, J., de Boisboissel, G. (eds.) *Robots on the Battlefield: Contemporary Issues and Implications for the Future*. Leavenworth, WA: US Army Combined Arms Center, Combat Studies Institute.

Trzun, Z., Vrdoljak, M. (2020) 'Monte Carlo Simulation of Missile Trajectories Dispersion due to Imperfectly Manufactured Warhead' in Katalinic, B. (ed.) *Proceedings of the 31st DAAAM International Symposium (pp. 0574-0583). Mostar, BiH, 21-24th October 2020*. Vienna: DAAAM International.

Trzun, Z., Vrdoljak, M., Cajner, H. (2021) 'The Effect of Manufacturing Quality on Rocket Precision', *Aerospace*, 8(6); https://doi.org/10.3390/aerospace8060160.

Tuchkov, V. (2016) 'VDV: "Andromeda-D" Will Support Strike Robots', *SvobodnayaPressa*, 27 January 2016. [Online]. Available at: https://svpressa.ru/war21/article/141023/ (Accessed: 5 January 2024).

U.S. Department of Defense (2022) *Civilian Harm Mitigation And Response Action Plan*. Washington, DC: Department of Defense.

Urcosta, R. (2018) 'Syria: Russia's Military Proving Ground', *US Naval Institute*, Proceedings, March 2018. [Online]. Available at: https://www.usni.org/magazines/proceedings/2018/march/syria-russias-military-proving-ground (Accessed: 30 October 2024).

Urmson, C., Anhalt, J., Bagnell, D., Baker, C. et al. (2009) 'Autonomous Driving in Urban Environments: Boss and the Urban Challenge' in Buehler, M., Iagnemma, K., Singh, S. (eds.) *The DARPA Urban Challenge: Autonomous Vehicles in City Traffic*. Heidelberg: Springer-Verlag, pp. 1-59; https://doi.org/10.1007/978-3-642-03991-1_1.

US Air Force (2021) 'MQ-9 Reaper', *Official US Air Force Website*. [Online]. Available at: https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/ (Accessed: 5 January 2024).

US Department of Defense (2005) *Unmanned Aircraft Systems Roadmap 2005-2030*. Washington, DC: Office of the Secretary of Defense.

US Department of Defense (2011) *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: US Department of Defense.

US Department of Defense (2021) 'Transcript: General Kenneth F. McKenzie Jr. Commander of U.S. Central Command and Pentagon Press Secretary John F. Kirby Hold a Press Briefing', 17 September 2021. [Online]. Available at: https://www.defense.gov/News/Transcripts/Transcript/Article/2780738/general-kenneth-f-mckenzie-jr-commander-of-us-central-command-and-pentagon-pres/ (Accessed: 5 January 2024).

Wall, P. (2013) 'Theory of the drone 12: 'Killing well'?', *Geographical Imaginations*, 8 December 2013. [Online]. Available at: https://geographicalimaginations.com/tag/hellfire-missile/ (Accessed: 5 January 2024).

Weinberger, S. (2008) 'Armed Robots Still in Iraq, But Grounded (Updated)', *Wired*, 15 April 2008. [Online]. Available at: https://www.wired.com/2008/04/armed-robots-st/ (Accessed: 5 January 2024).

Werner, A., Kreutzmann, U., Glowka, S., Schinkel, C. (2020) 'The New Quality of Aviation Unmanned Aerial Vehicles (UAV) Prevent Psychological Stress of Military Drone Operators', *Clinical Medicine Research*, 9(1), pp. 25–30; https://doi.org/10.11648/j.cmr.20200901.15.

Whitlock, C. (2014) 'When Drones Fall from The Sky', *The Washington Post*, 20 June 2014. [Online]. Available at: https://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/ (Accessed: 5 January 2024).

Wu, M. (2022) *Intelligent Warfare: Prospects of Military Development in the Age of AI*. New York, NY: Routledge, Taylor and Francis Group; https://doi.org/10.4324/b22974.

Xiao, X., Dufek, J., Murphy, R.R. (2021) 'Autonomous Visual Assistance For Robot Operations Using A Tethered UAV' in Ishigami, G., Yoshida, K. (eds.) *Field and Service Robotics: Results of the 12th International Conference*. Singapore: Springer Singapore, pp. 15–29; https://doi.org/10.1007/978-981-15-9460-1_2.

Yamauchi, B. (2004) 'PackBot: A versatile platform for military robotics' in *Defense And Security, SPIE Proceedings, (Vol. 5422). Orlando, FL, US, 12-16 April 2004*. Bellingham, WA: SPIE, pp. 228–237; https://doi.org/10.1117/12.538328.

A-10 And MQ-9 In ICT Operation | Finland Closer To Buying David's Sling | Denmark Gets New Howitzers (2023) *Defense Industry Daily*. [Online]. Available at: https://www.defenseindustrydaily.com/a-10-and-mq-9-in-ict-operation-finland-closer-to-buying-davids-sling-denmark-gets-new-howitzers-048238/ (Accessed: 5 January 2024).

Drone Crash Database (2022) *Drone Wars UK*. [Online]. Available at: https://dronewars.net/drone-crash-database/ (Accessed: 5 January 2024).

Lynx Multi-Mode Radar: Surveillance, Tracking, Targeting for Manned and Unmanned Missions (no date) *General Atomics Aeronautical*. [Online]. Available at: https://www.ga-asi.com/radars/lynx-multi-mode-radar (Accessed: 5 January 2024).

MQ-9 Reaper (no date) *Air and Space Forces Magazine*, no date. [Online]. Available at: https://www.airandspaceforces.com/weapons-platforms/mq-9/ (Accessed: 5 January 2024).

Predator B Extended Range Conducts First Flight With Long Wings (2016) *General Atomics Aeronautical*, 25 February 2016. [Online]. Available at: https://www.ga-asi.com/predator-b-extended-range-conducts-first-flight-with-long-wings (Accessed: 5 January 2024).

Record number of US drone crashes (2016) *BBC News* 21 January 2016. [Online]. Available at: https://www.bbc.com/news/technology-35370262 (Accessed: 5 January 2024).

Russia is starting to make its superiority in electronic warfare count (2023) *The Economist*, 23 November 2023. [Online]. Available at: https://www.economist.com/europe/2023/11/23/russia-is-starting-to-make-its-superiority-in-electronic-warfare-count (Accessed: 5 January 2024).

TALON Tracked Military Robot (2020) *Army Technology*, 21 February 2020. [Online]. Available at: https://www.army-technology.com/projects/talon-tracked-military-robot/?cf-view (Accessed: 5 January 2024).

Chapter 13

Legal Aspects of Unmanned Warfare and Military Drone Operations

Kaja Kowalczewska

Abstract

The evolving landscape of warfare has been transformed by the technological advancement of unmanned platforms. The use of drones has facilitated the remote execution of military operations, allowing armed conflict to achieve a global and presumably selective scope through sophisticated technological organisation. Nevertheless, the past two decades of mainly American practices have revealed that so-called "precision warfare" poses novel ethical and legal challenges. Despite the multifaceted roles played by contemporary military robots, especially in scenarios where they replace human combatants and execute lethal actions, comprehensive legal scrutiny is imperative.

Although unmanned platforms do not attain the same level of autonomy as military systems enabled by artificial intelligence, they still present challenges. In the case of unmanned platforms, the contentious aspects predominantly relate to their methods of employment rather than the inherent illegality of this means of warfare. This chapter critically dissects the legal complexities surrounding these technological innovations, distinguishing drones from autonomous weapons and examining their deployment methods and the relevant legal framework.

Key issues include the necessity for legal review of weapons before deployment, the use of unmanned platforms beyond the theatre of active armed conflict, and contentious combat methods such as targeted killings and signature strikes. While predominant discussions centre on U.S. drone warfare, this chapter incorporates a European perspective where relevant, highlighting the need for harmonisation of democratic standards.

Kaja Kowalczewska (2024) 'Legal Aspects of Unmanned Warfare and Military Drone Operations'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 581–615. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_13

Keywords: unmanned platforms, drone warfare, use of force, law of armed conflict, international human rights law, drone policy

1. Introduction

In the ever-evolving landscape of warfare, the introduction of unmanned platforms is a significant technological leap. This chapter scrutinises the legal intricacies of these innovations, aiming to unravel the implications of their deployment. While drones are often lumped together with autonomous weapons, it is crucial to define the differences. This chapter elucidates why the legal dilemmas surrounding unmanned platforms, especially within drone warfare involving targeted killings and signature strikes, demand critical examination.

While discussions and analyses are predominantly around the experiences and surrounding U.S. drone warfare, the focus is also directed towards the European approach towards military drone technologies, ensuring a comprehensive understanding of diverse perspectives.

This chapter begins by defining key terms pertaining to unmanned platforms, distinguishing them from autonomous weapons. It then examines the history of drones in military operations and legal reviews of new weapons. Further, it explores the use of unmanned platforms within and outside armed conflicts, including the rise of drone warfare, the controversies surrounding targeted killings, and the challenges posed by these precision strikes. It also investigates the subject of responsibility in drone operations, considering both state and individual accountability. The chapter culminates by underscoring the imperative of formulating a unified European strategy to effectively manage and regulate the utilisation of military drones. This necessitates consideration within European policy frameworks of the legal, ethical, and policy dilemmas inherently associated with these technologies within the contemporary landscape of warfare.

2. Legal Definitions

2.1. Robots, Drones, and Unmanned Platforms: Defining the Terminology

The terms “military robots” and “drones” conjure images that are no longer confined to the realm of science fiction. It is widely acknowledged that a robot can receive information from its surroundings and independently carry out specific physical

actions through a controller and system.[1] This implies that a robot has a supportive and subordinate role to humans. This is precisely how Karel Čapek, the originator of the term "robot", portrayed them as far back as 1920. In the military context, contemporary robots fulfil a diverse array of functions, that at the moment, are mainly confined to supportive tasks. This is why it is important to present the various tasks that are already being performed by robots in a military context, clarify the associated vocabulary, and delineate the legal challenges and consequences related to the legality of their use and the legal consequences of their use.

Transport (logistics) robots play a crucial role in moving people, including disaster victims and those injured during hostilities, as well as equipment that is beyond human capacity to transport, such as various types of ammunition and supplies. Robots are also instrumental in locating and disarming explosive devices, making them valuable assets in clearing minefields and removing dangerous obstacles. Furthermore, robots contribute to surveillance and reconnaissance, penetrating enemy lines to identify potential threats. Robotic systems are also employed in personnel training, enabling the recreation of operational environments without exposing individuals to additional risk. However, the most commonly cited military application of robots undoubtedly pertains to their lethal capacity, which involves the ability to engage kinetically with any object or individual.

The examples of robots mentioned above and described in more detail in Chapter 12 showcase their diverse functions. However, their classification can be expanded based on their operational domain (aerial, terrestrial, underwater, or cybernetic), their resemblance to humans or animals, or any shape. Furthermore, they can be evaluated based on whether they are manned or unmanned. The most critical and existential debate revolves around whether they replace or support humans, and more crucially, in which specific tasks they do so.[2] All these attributes impact every stage in the lifecycle of a robot, from its inception and production to its deployment in military settings, its use in combat scenarios, and the assessment of its legality and potential liability for any unlawful actions involving the technology.[3]

Considering the scope of this chapter, a comprehensive analysis of all the challenges and issues associated with every robot model is not feasible. Instead, the focus will be on a specific subgroup of robots, which are distinguished by their lethal capabilities, unmanned nature and their human-supportive rather than human-substitute roles. It is within this category of military robots that numerous legal and ethical questions arise, warranting in-depth examination by lawyers and ethicists.

Before delving into the legal analysis, it is imperative to establish clear definitions for common terms used in discussions regarding military robots. After all, the lawyer's primary tool is language, as it shapes the reality being examined. While military robots and drones are common subjects in doctrinal considerations, international

1 ISO, 2012.
2 Bober, 2015, pp. 32–47.
3 Copeland, Liivoja and Sanders, 2023, p. 294.

legal definitions for the terms ‘drones’ and ‘military robots’ are lacking. Therefore, it is essential to clarify that throughout this discussion, terms such as military robots, drones, and unmanned platforms, including unmanned airborne vehicles (UAVs,) unmanned ground vehicles (UGVs), and unmanned underwater vehicles (UUVs) will be used interchangeably. Where relevant, the appropriate national regulations will be cited; otherwise, this analysis is solely focused on international law.

Beyond the terms previously mentioned, there exist additional concepts that necessitate clarification for legal analysis. A common misconception that arises in public discourse on drones is the use of the term “unmanned systems”, which should be more accurately referred to as “unmanned platforms”. A useful standard of reference here is the NATO glossary (AAP-06), which contains definitions to which all Member States have agreed.[4] The term “weapon systems” emphasises that technology or weaponry does not operate in isolation.[5] Therefore, achieving “weapon system self-sufficiency” entails combining the requisite equipment, materials, personnel, and means of installation and delivery necessary for its autonomous operation. The concept of a system also encompasses human involvement, which is particularly pertinent when characterising these systems as “unmanned”.

Consequently, an “unmanned system” is an unmanned platform with the necessary equipment, communications, software, and personnel for remote control or supervision.[6] The illustration provided in Chapter 12 regarding the Reaper system encompasses various elements, such as the ground control station, line-of-sight and beyond-line-of-sight satellites, terrestrial data links, support equipment and deployed personnel. Another essential point requiring clarification in the term “unmanned” is whether it signifies the absence of a physical human presence on the platform or system or the absence of human control, irrespective of physical presence. Adopting the latter definition has led to the following definitions:

- Human-in-the-loop weapons (a human in the process): In this category, a robot can only select a target and use force when directed by a human operator.
- Human-on-the-loop weapons (a human above the process): Robots can select a target and use force under human supervision. The human operator holds the authority to override the robot’s decisions.
- Human-out-of-the-loop weapons (there are no humans in the process): Robots can autonomously select targets and employ force without human intervention.[7]

While not without limitations, especially considering the delicate balance between the human capacity to swiftly react and override robot decisions (human-on-the-loop)

4 NATO, 2021.

5 A combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment, if applicable, required for self-sufficiency. Ibid.

6 A system whose components include the unmanned aircraft, the supporting network and all equipment and personnel necessary to control the unmanned aircraft. Ibid.

7 Human Rights Watch, 2012, p. 2.

versus the absence of such control (human-out-of-the-loop), this framework aids in categorising human-robot interactions. This categorisation is significant because, in the context of such weaponry, there are legal considerations around the role of humans as the recipients of legal norms and their consequent place in the loop. These circumstances stem from at least three key factors. First, robots are not yet recognised as legal entities subject to the law. Second, there is no specific international treaty that explicitly prohibits or restricts their use, unlike those regulating anti-personnel mines and chemical or nuclear weapons. Third, the human role in human-robot interactions is crucial from both ethical and legal points of view, particularly regarding criminal responsibility.

Consequently, the legal analysis of military robots relies on interpreting the collective body of legal norms applicable to their deployment. This includes fundamental areas of international law, such as the use of force, the law of armed conflict (LOAC), international human rights law (IHRL), and international criminal law.

2.2. Unmanned Platforms versus Autonomous Weapon Systems

In the following analysis, it is imperative to distinguish between autonomous military robots that can replace humans and those in which human involvement remains a factor. This differentiation arises not only from technological advancements, such as equipping these machines with artificial intelligence (AI), but also from a distinction in the fundamental nature of these weapons. Given that unmanned platforms are capable of delivering kinetic force, the legal and ethical considerations hinge on whether these robots are remotely guided or operated in real-time by a human or if they are controlled by AI. The division of human in/on/out of the loop mentioned earlier exists to categorise military robots precisely because of this issue.

An alternative framework involves classifying weapons as automatic, automated, or autonomous. In this context, the emphasis is not on the human-robot relationship but rather on the predictability of the weapon's behaviour.[8] In automatic systems, future actions are predictable as they are programmed to react consistently to a given stimulus (for example, anti-personnel mines). In automated systems, the scope of action is expanded but remains limited to situations where actions have been pre-programmed (e.g., the early self-driving cars). Finally, in autonomous systems, the outcomes of actions are unpredictable because of their ability to make decisions in variable and complex environments (e.g. the AI's "black box").

Hence, the crux of the matter concerning military robots and autonomous weapon systems is human control, which can be understood as either remote control or the assurance of high predictability in the systems' actions. It is worth noting that the boundary between these two categories is quite fluid (a technological continuum), as the manner in which robots are operated can significantly impact the quality of

8 Development, Concepts and Doctrine Centre, 2022, p. 11.

the human-robot interaction.[9] Some of the most frequently mentioned challenges include confirmation bias[10] or the "android fallacy", characterised by excessive reliance on information from sensor systems and information analysis, as well as the illusory nature of remote control, particularly when overseeing a swarm of robots simultaneously (like Sparrowhawks mentioned in Chapter 12), which can lead to task monotony and slower response times.[11] As a result, discussions on autonomous weapons systems, particularly within the framework of the Convention on Certain Conventional Weapons in Geneva, emphasise the concept of "meaningful human control" as a prerequisite for the deployment of such systems and an important factor in attributing individual responsibility for violation of the LOAC.[12]

Hence, in the case of military robots that are remotely controlled or highly predictable, the issues surrounding whether their actions align with LOAC and IHRL[13] and the issue of the "accountability gap" (the challenge of assigning responsibility for law violations using these technologies to a specific individual) are less prominent.[14] It appears that the matter of remotely controlled and predictable military robots is comparatively more straightforward. Nevertheless, this does not imply that it is without challenges. These types of technologies, unlike autonomous ones, have been in use on the battlefields since the early 21st century and the practical application of these technologies has raised numerous legal questions, which will be explored in this chapter.

3. Introduction of Drones to the Armed Forces

3.1. Means and Methods of Warfare: Understanding the Context

A historical analysis of the rationales and methods of weapons regulation reveals that states are motivated by both humanitarian and practical considerations. On the one hand, weapons that inflict excessive suffering, such as blinding laser weapons or weapons of mass destruction, are prohibited. On the other hand, extra-legal factors, such as safeguarding public safety, protecting the strategic interests of arms manufacturers and users, and sustaining arms races, sometimes lead to the absence of regulation or dual-track regulation, as seen in cases like anti-personnel mines and cluster munitions. As Sean Watts aptly points out, weapons can be categorised as

9 Kate-Devitt, 2018, pp. 161–184.
10 Mentioned in the case of the use of a MQ-9 Reaper in Afghanistan on 29 August 2021, in Chapter 12.
11 Richards and Smart, 2016, pp. 18–21.
12 Moyes, 2016; Santoni De Sio and Van Den Hoven, 2018, p. 15; Acquaviva, 2023.
13 Human Rights Watch, 2012.
14 Human Rights Watch, 2015.

either regulation-tolerant or regulation-resistant.[15] It is the latter group, characterised by their military utility, effectiveness, novelty, and disruptiveness, that is reluctantly regulated, especially by military powers.

Consequently, it can be argued that military robots, due to their distinctive characteristics (presented in Chapter 12), fall into the category of regulation-resistant weapons, akin to nuclear weapons, submarines, firearms, and ammunition. With the absence of specific legislation and minimal prospects for its enactment, an analysis of the legality surrounding the development and use of military robots necessitates the identification of the most relevant general regulations that provide guidance on the norms governing these processes.

A crucial foundational concept is the definition of *weapons*. Treaty norms and customary international law lack a specific definition for weapons, which underscores the pivotal role of doctrine in this regard. From a practical perspective, weapons are tools employed by individuals to surpass their physical or mental limitations in combat. A weapon is essentially a means of combat used during warfare. In this context, means of combat includes firearms, rockets, bombs, or other munitions capable of causing death or injury to individuals or destroying or damaging objects.[16] Weapons can exert force through kinetic means or through the transmission of electrical energy, the dispersion of chemical substances biological agents, through sound, through manipulation of electromagnetic energy, or the generation of effects in cyberspace.

The terms "means of warfare", "means of combat", "means of attack", and "weapons" are interchangeably used in doctrine and international agreements concerning arms.[17] In practice, "means of combat" is the prevailing concept in LOAC doctrine, while the term "weapons" is more commonly found in disarmament and arms control agreements. "Means of combat" is a broader yet more precise concept than "weapons", as it encompasses not only arms used in armed conflicts but also weapons platforms and systems employed by parties engaged in hostilities. Consequently, it does not pertain to arms used in crowd control, for instance, or by state security authorities.

Doctrine distinguishes between "means of combat" as pieces of equipment, such as ammunition, substances or objects, and "weapons", which refer to the actual capability used to incapacitate or reduce a military target's effectiveness, rendering individuals unable to effectively participate in combat. Another concept often associated with weapons and means of warfare is "methods of warfare", which are ways a particular weapon or means of combat may be employed during military actions or

15 Watts, 2015, pp. 540–621.

16 The Program on Humanitarian Policy and Conflict Research, 2013, p. 16.

17 Article 1 of the Treaty on the Non-Proliferation of Nuclear Weapons, 1968; Article 1 of the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, 1972; Articles 35, 36, 51 and 57 of Additional Protocol (I) to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts, 1977 (AP I).

the strategies or tactics used. However, the international legal framework also lacks a specific definition for methods of warfare, and doctrine tends to examine them only infrequently.

Military robots are commonly categorised as weapon platforms and systems rather than specific types of weapons. After all, a robot can be equipped with various types of weapons and ammunition (for example, the MQ-9 Reaper has AGM-114 Hellfire guided missiles and GBU-12 Paveway II bombs). An essential distinction with military robots is they are remote controlled and unmanned. The term "drone warfare" has already emerged as a method of warfare conducted using remotely controlled UAVs. Consequently, the central focus of this chapter is not solely on the legality of military robots as a means of warfare but rather on the legality of the way in which they are utilised as a method of warfare. This, of course, does not exclude the legality of the weapons specifically utilised by military robots, but this issue is beyond the scope of the research presented in this chapter.

3.2. Legal Review: Ensuring Compliance

Contrary to common belief, new military technologies do not operate in a legal void. While it is true that international law often lags behind the development and deployment of technologies, which are typically created, used, and only then subject to regulation (potentially through complete bans or limitations on their use), international law does take these possibilities into account. This is primarily accomplished through the application of fundamental principles of LOAC, such as the limited right to select means and methods of warfare, the prohibition of superfluous injury or unnecessary suffering, the prohibition of extensive, enduring and severe harm to the natural environment, and the principles of distinction, precautions, and proportionality.[18] A pivotal provision that plays a preventive role, anchored in these principles, is art. 36 AP I:

> Article 36 – New weapons. In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

In simpler terms, this regulation places a responsibility on States Parties to consistently ensure that the weapons they procure and the methods of warfare they develop align with the stipulations of AP I, as well as a range of other relevant international legal norms applicable to the circumstances of their use.

At the outset, it is crucial to delineate the nature of this provision. It is a treaty norm that has not been subject to reservations or declarations and, therefore, is

18 Hagger and McCormack, 2012, pp. 1–26.

binding on all 174 States Parties, which include all Member States of the European Union (EU). Furthermore, as emphasised by Natalia Jevglevskaja, there is no consistent and established state practice (*usus*) despite the recognition of the provision's enforceability as law (*opinio juris*), and, as a result, this norm has not attained customary status.[19] However, it is noteworthy that certain states like the United States (a signatory state) or Israel (not even a signatory state) conduct legal reviews based on their domestic laws. What adds further significance to this is that based on available information (since there is no requirement to publicly disclose the conduct of a legal review), only around 20 states globally undertake such reviews.[20] This raises questions about the effectiveness of this provision. Nevertheless, in the discourse on autonomous weapon systems, the matter of legal review has experienced a resurgence, as states consider this process as a means to address the legality of disruptive weapons.[21]

3.2.1. Scope and Standards of Legal Review

It is essential to consider the following issues concerning the legal review process: the material and normative scope of the review, the timing at which the obligation is activated, and procedural considerations. Given the ambiguity of art. 36 AP I and the lack of comprehensive international legal regulations on the matter, this analysis is based on best practices advocated by the International Committee of the Red Cross (ICRC) and drawn from operational national procedures.[22]

The complexity of legal reviews is contingent upon the sophistication of the subject under examination. While it is reasonable to assume that evaluating the legality of firearms is relatively straightforward, assessing the legality of military robots, especially autonomous ones, demands a more intricate and resource-intensive analysis. Here, it is important to emphasise that states are only required to scrutinise whether the typical and anticipated use of a particular weapon could be prohibited under any circumstances.[23] A legal review cannot reasonably cover all conceivable misuse scenarios, as that would render the study unfeasible. Any weapon (or object) can be employed in ways that breach legal norms. Therefore, a critical element of the examination involves characterising the means of warfare, such as a military robot, encompassing its inherent functions and intended purposes (method of warfare). These aspects establish the parameters for the scenarios within the legal review.

Despite the title of art. 36 AP I, the obligation to conduct a legal review is not applicable to every newly introduced weapon in the market. The notion of novelty, in this context, pertains to the standpoint of a state developing or acquiring the specific

19 Jevglevskaja, 2018, pp. 186–221.
20 Jevglevskaja and Liivoja, no date.
21 Copeland, Liivoja and Sanders, 2023, pp. 285–316.
22 ICRC, 2006.
23 Sandoz, Swiniarski and Zimmermann, 1987, para. 1469.

means or method of warfare in question. This includes conventional weapons, which were the primary focus of the AP I, but also extends to novel types of weaponry, following the wisdom that '[i]f humans do not master technology but allow it to master them, they will be destroyed by technology'.[24]

This matter is intertwined with the normative scope of the review. The language of art. 36 AP I makes it evident that the legal review must consider the provisions of AP I, with particular emphasis on art. 35 AP I. Furthermore, it should encompass other pertinent international laws that are applicable to the state and subject of the review. In particular, it is advisable to adopt a multidisciplinary approach that takes into consideration safety, environmental impact, health, human rights, and administrative regulations concerning matters such as registration, transportation, and insurance of the subject of the review.[25] As a result, it has been recommended that the team responsible for the legal review should comprise specialists with diverse backgrounds, including military experts, engineers, lawyers, psychologists and medical professionals. It cannot be ruled out that ongoing cooperation with the manufacturer's representatives will be necessary with more technically advanced weapon systems. This collaboration would aim to adequately assess the robot's suitability and to tailor the methods and scope of end-user training, or define specific conditions linked to updating and maintaining it.

For older or well-established weapons, the legal review process is relatively straightforward, as it primarily involves an analysis of existing international agreements to determine whether a specific means of warfare is prohibited or restricted by these agreements. In contrast, when dealing with newer means of warfare, such as military robots, dedicated international standards are lacking. Therefore, the legal analysis relies primarily on the interpretation of existing general standards, especially the fundamental principles of the LOAC, resulting in potential variations in assessments by individual states. It is important to note that in the case of military robots, the evaluation primarily focuses on their intended purpose and methods of use, as the design of the platform itself does not inherently pose legal challenges.

The above is significant because only a limited group of military powers are weapon-producing states, and others procure weapons from these producers. Consequently, a situation may arise where a producer state (e.g., the United States) may assert that a specific weapon complies with the applicable international laws. However, this assertion may not hold true for the acquiring state. A prime example of this is the cooperation among NATO member states, which include EU Member States and the United States, among others.[26] Due to variations in states' international legal obligations (stemming from differences in the ratification of various international agreements), they may not always be able to act uniformly in a combat environment. Within the context of European States, a notable distinction arises from the

24 Ibid., para. 1746.
25 ICRC, 2006, p. 935.
26 Olson, 2013, pp. 653–657; Abbott, 2014, pp. 107–137.

regional human rights protection system, with the European Court of Human Rights at its core. This system places additional obligations on these states, particularly concerning IHRL standards on the methods of warfare employed. Added to this, the lack of transparency and public disclosure of review methods, the absence of standardisation and divergent scopes regarding international legal obligations significantly impact interoperability. Consequently, the obligation to conduct a legal review is tailored to each manufacturing, purchaser, or user state. If any modifications or enhancements are made to a robot, a legal assessment of its legality must be re-conducted to evaluate the implications of such alterations.

Notably, aside from the legal aspects, there is no consensus regarding whether the subject of the review should also be assessed in terms of the *Martens clause*,[27] which is: the 'principles of humanity and requirements of public conscience'.[28] The author holds the view that such an ethically-oriented approach is acceptable, and this viewpoint is confirmed in the practices of states such as Australia and the United Kingdom. In essence, invoking the ethical dimension and assessing the desirability of developing a specific means or method of warfare can methodologically strengthen a state's ultimate decision on whether to engage in research or incorporate a particular means or method of warfare into its armed forces' arsenal.[29] It is worth noting that the Martens clause frequently arises in discussions regarding autonomous weapons systems, and it can also be a significant reference point in the context of drone warfare.

Regarding procedural aspects, the review team should be chosen on a case-by-case basis, taking into account the specific challenges associated with the subject of the review. There are a few key points from good practice that states should consider. The ICRC recommends that a responsible authority, whether within the political or military state structures, be designated to oversee the review[30] and should establish a clear trigger point for the procedure's implementation, introduce appropriate documentation, and establish rules for making the final decision. The outcome of the review can be presented in the form of a report, which should indicate whether a particular measure or method of combat is deemed acceptable and, if so, specify the situations in which the state should refrain from using it and outline the necessary precautions. While there is no obligation to publicly disclose the results of the review, considering the strategic interests of states and the necessity of maintaining military capabilities as classified information, the ICRC advocates for at least a partial release of such a report or the establishment of an international body to oversee the transparency and integrity of national review procedures. A similar demand has also been recently made in the context of autonomous weapon systems.[31]

27 Art. 1 (2) AP I.
28 Meron, 2000, pp. 78–89.
29 ICRC, 2006, p. 945.
30 Ibid., p. 949.
31 Argentina, 2019.

3.2.2. EU's Unique Approach

Given the lack of domestic legal reviews, despite the international legal obligation to conduct them, with only a few cases documented based on publicly available data, this study strongly recommends the establishment, maintenance, and regular update of such procedures, especially in those states bound to do so by AP I. This recommendation extends to the EU Member States, which are founded on democratic principles, including the rule of law, and are expected to conduct these processes diligently. Among the 27 EU Member States, only 12 have disclosed that they are conducting legal reviews. These states are Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Ireland, Italy, the Netherlands, and Sweden.[32] Therefore, when urging the other 16 domestic governments of European nations to fulfil their international legal obligations, it is worth presenting a general comparative overview of procedures practiced in other EU Member States.

EU Member States commonly delegate the responsibility for legal reviews to military-associated entities, primarily housed within defence ministries or directly within armed forces. However, Sweden stands out as an exception, leading the way in establishing an independent delegation appointed by the government and operating autonomously outside these structures since as early as 1974. In Italy, the review team includes representatives from the Ministry of Defence and both houses of Parliament. The overseeing body is often interdisciplinary and multidisciplinary, with potential for the inclusion of external experts.

With the exception of Sweden, where the delegation conducting legal reviews convenes three or four times annually, most procedures are *ad hoc* but initiated at the earliest stages of acquiring or developing means or methods of warfare. This typically happens prior to issuing a tender or signing a contract, as seen in Denmark and the Netherlands.

The outcomes of the legal review typically result in internal reports providing advice or recommendations, except in the Netherlands, where they hold binding authority. Accessibility and transparency of the review varies across states. Generally, the findings are not considered public. However, in specific states, such as Italy and Sweden, they are treated as partially accessible to the public.

The exposition of commonalities underscores that EU Member States engaged in legal reviews have achieved a minimal but uncoordinated level of harmonisation. The exercise of such actions distinctly pertains to the exclusive competence of sovereign states, rendering advocacy for overarching harmonisation presently unfeasible. However, it is important to note that 23 EU Member States are also NATO members. This affiliation strengthens the case for effectively enforcing art. 36 AP I, driven by political, military, and economic considerations. In cases involving advanced systems, such as military robots, where joint coordination, data sharing, and

32 Farrant and Ford, 2017, p. 391; Jevglevskaja, 2018, p. 192.

collaborative programmes are essential, establishing standardised procedures at a basic level becomes crucial.

4. Use of Drones

The integration of unmanned platforms, specifically aerial ones, has revealed challenges in implementing international legal norms, particularly those governing the use of force (*jus ad bellum*) and LOAC (*jus in bello*). The introduction of these technologies has functioned as a lens, highlighting and magnifying the complexities associated with interpreting and applying these legal frameworks.

4.1. Use of Unmanned Platforms outside Armed Conflicts

In the context of the use of force, a crucial aspect is the utilisation of unmanned platforms in settings removed from active armed conflicts. This detachment refers to their deployment in geographical areas where there is no ground-based combat or in situations where there are no ongoing armed conflicts. This includes instances where states opt for UAV-led attacks without deploying troops for a full-scale mission in the field. Put differently, it specifically pertains to employing force through targeted killings.

4.1.1. The Rise of Drone Warfare and Targeted Killings

The 21st century has witnessed a surge in targeted killings, a practice previously associated with special forces missions.[33] Traditionally, these missions involved specific forces being dispatched to eliminate a particular adversary and then returning to base. These operations typically cross borders, occurring on the territory of another state; however, the advent of UAV technology has transformed these missions into fully unmanned operations. In this evolution, the UAV operator remains within their home state's territory while directing the UAV abroad to execute its intended action. According to Philip Alston, Special Rapporteur on extrajudicial, summary or arbitrary executions,

> (…) a targeted killing is the intentional, premeditated and deliberate use of lethal force by States or their agents acting under colour of law, or by an organized armed group in armed conflict, against a specific individual who is not in the physical custody of the perpetrator.[34]

33 Blum and Heymann, 2013, pp. 69–92.
34 HRC, 2010, para. 1.

Examples include the operation that led to the killing of Osama Bin Laden in Abbottabad, Pakistan (April 2011), the shelling of a column near Sirte in Libya, resulting in the death of Muammar Gaddafi (October 2011), and the incidents involving Qasem Soleimani in Baghdad (January 2020) and Ayman Al-Zawahiri in Kabul (July 2022).

The widespread use of UAVs for targeted killings is commonly associated with the aftermath of the 9/11 attacks and the subsequent 'war on terror' within the asymmetric warfare paradigm. However, this approach results in misinterpretations of legal principles and breaches of IHRL standards, leading to adverse consequences such as the proliferation of terrorist organisations, diminished security for populations, and widespread public backlash.[35]

An aspect not directly within the realm of international law but rather concerning domestic law involves the process of consent for drone usage. As highlighted by Milena Sterio, consolidating these decision-making powers within a single office or branch of government can pave the way for potential abuse.[36] In the instance of the attack on Soleimani, the U.S. President used independent domestic legal authority to employ military force overseas, bypassing Congress and executing an operation that significantly raised the probability of engaging in armed conflict with Iran.[37] Indeed, a crucial aspect of drone warfare is how relatively easy it is for decision-makers to employ them for attacks. Unlike sending soldiers who face potential danger and may not return, drones are costly military equipment supposedly designed for surgical precision in their attacks.[38] This characteristic is marketed to the decision-makers as a less risky option when engaging in use of lethal force. As it happens, and as will be discussed below, this turns out to be a myth.[39]

The described characteristics have rendered drone warfare an exceedingly attractive alternative to conventional warfare.[40] With a focus on minimising self-inflicted losses and leveraging technological superiority, drones promise heightened effectiveness and the reduction of collateral damage. Therefore, states have progressively expanded their arsenals by developing and deploying new UAV models.[41]

Unfortunately, certain drone programmes, notably those overseen by entities such as the CIA, have been conducted clandestinely.[42] The use of clandestine drone operations hampers the possibility of subjecting this method of warfare and its individual operations to thorough legal scrutiny and evaluation.[43] Consequently, a substantial part of drone warfare policy is veiled in secrecy despite over ten states

35 Walsh, 2015, pp. 507–523; Coyne and Hall, 2018, pp. 51–67.
36 Sterio, 2018, pp. 35–50.
37 Anderson, 2020.
38 White House, 2013.
39 HRC, 2020, paras. 15–21; Khan, 2021.
40 Walsh and Schulzke, 2015.
41 DroneWars.net, 2023.
42 Lubold and Harris, 2017.
43 Blum and Heymann, 2013, pp. 69–92.

utilising UAVs for such purposes and several others possessing these systems in their military inventory.[44]

4.1.2. Use of Lethal Force via Unmanned Platforms

The laws governing the use of force are shaped by customary and treaty norms that delineate the circumstances under which states can lawfully utilise force in international relations. Until 1928, warfare was perceived as a means of settling disputes. However, with the adoption of the Briand-Kellogg Pact,[45] a significant shift occurred. Article I of the pact condemns the use of war to resolve international controversies and renounces it as a tool of national policy in state relations. While this commitment did not withstand the test of the Second World War, it gained significant reinforcement afterward.

The quest for peace and condemnation of aggressive warfare became foundational principles within the United Nations (UN). The UN Security Council (UNSC) has the 'primary responsibility for the maintenance of international peace and security' (Art. 24 of the UN Charter), and the obligation to 'determine the existence of any threat to the peace, breach of the peace, or act of aggression (…)' (Art. 39 of the UN Charter).[46] The prohibition of the use of force is embodied in Art. 2(4) of the UN Charter, which explicitly prohibits 'the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations'. This provision underscores the fundamental values of sovereignty, political independence (embodying the principle of non-intervention), and territorial integrity,[47] safeguarded within the contemporary international legal framework. Indeed, the definition of an act of aggression was adopted by the General Assembly through Resolution 3314 in 1974.[48] Furthermore, within the realm of international criminal law, aggression has been recognised as an international crime, detailed in art. 8bis of the Rome Statute.[49] Thus, any breach of these principles through the utilisation of military force can result in states being held accountable for internationally wrongful acts under ARSIWA,[50] whereas individuals may be judged accountable by the International Criminal Court or domestic courts.[51] In both scenarios, the use of a military UAV could be categorised as an act

44 NewAmercia.org, no date.

45 *The General Treaty for Renunciation of War as an Instrument of National Policy*, 1928.

46 *The Charter of the United Nations*, 1945.

47 In this context, it is important to note that airspace constitutes an integral part of a state's territory. Therefore, any infringement upon it could be considered a violation.

48 UNGA, 1974.

49 *Rome Statute of the International Criminal Court*, 1998.

50 *Articles on Responsibility of States for Internationally Wrongful Acts*, 2001.

51 The history of the 20th and 21st centuries bears witness to violations of this prohibition; however, these transgressions do not nullify its application. Recent events, particularly Russia's overt aggression against Ukraine on 24 February 2022, have revitalized discussions surrounding the crime of aggression, prompting renewed scrutiny.

or crime of aggression. The declaration of war becomes irrelevant in this context. What matters is that State A is invading or attacking State B's territory using armed forces such as UAVs, UUVs UGVs or any other weapon.

In regard to *jus ad bellum*, unmanned platforms serve as a means through which the use of force can be executed. However, their unique characteristics, especially their remote attack capabilities, have exacerbated tensions surrounding previously contentious doctrines. The advent of drone use has made the use of lethal force more cost-effective, quicker, and simpler. Consequently, we are witnessing numerous brief violations of the prohibition on the use of force in interstate relations that are sometimes challenging to assess. The imperative to combat terrorist organisations has further fuelled the surge in such instances, with targeted killings proving to be an effective method in pursuit of this goal.

The prohibition on the use of force typically allows for only two exceptions. The first exception involves a state invoking its inherent right to self-defence, a principle deeply rooted in customary law and explicitly recognised in art. 51 of the UN Charter. The second exception is the use of military force based on authorisation by the UNSC under Chapter VII of the UN Charter. For a state to lawfully use force, it must either act with another state's consent or adhere to the cited exceptions – authorisation by the UNSC or the right of self-defence. To invoke the latter, a state must first be the victim of an armed attack, then officially notify the UNSC which should take action necessary to maintain international peace and security. The prevailing stance is that any action involving the use of force in interstate relations should adhere to the principles of proportionality, determining the extent and type of force permissible and necessity, and ensuring that force is employed as a last resort. However, with the proliferation of UAVs, an alternative perspective has gained prominence. The concept of pre-emptive self-defence lacks direct justification in the treaty law as Art. 51 of the UN Charter clearly stipulates that an armed attack must occur to trigger the right to self-defence. However, ongoing doctrinal debates persist regarding the legitimacy and extent of military action aimed at prevention and mitigation of potential harm. Furthermore, in its most recent report, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism accepted that

> (…) the dominant contemporary international position is that the use of lethal force in anticipatory self-defence by a State may be lawful so long as it responds to an *imminent* threatened armed attack, and where that response is necessary and proportionate.[52]

The proliferation of UAVs has significantly heightened the ongoing debate, particularly focusing on the concept of 'imminency' within legal contexts.[53] While these

52 HRC, 2022, p. 11.
53 Brooks, 2014, pp. 93–94.

drones offer a technological solution that streamlines actions and reduces adverse consequences, there's apprehension about their potential to establish risky legal precedents and expand justifications for employing force within the realm of international law.

Moreover, the UN Charter does not explicitly address armed attacks conducted by non-state actors (such as terrorist organisations). However, it is now widely accepted that states have the right to invoke self-defence in response to such attacks[54] which leads to another legal dilemma. It is acknowledged that using force on another state's territory with its explicit consent is a straightforward scenario. However, the situation becomes considerably more complex when the territorial state remains silent, exhibits hostility, or fails to respond in any way. The right to use force within the territory of a state when that state is unwilling or unable to prevent an attack by a non-state actor is a contentious issue. While some states support this right,[55] the principle faces strong condemnation within academic circles.[56] In the Special Rapporteur's view, when a non-state actor operates independently from the territorial state's control or when the actions of these actors cannot be attributed to that state under ARSIWA, a state sending a drone to neutralise that non-state actor would violate both the prohibition of the use force and the principle of state sovereignty.[57]

In principle, the UNSC should be notified of any use of force under the self-defence principle. However, these notifications are often superficial, and the legal justifications they provide in them can be contentious. There have been instances where states have unlawfully stretched interpretations of UNSC resolutions, expanding their scope. For example, UNSC Resolution 2249 did not authorise intervention in Syria without the consent of the Syrian government.[58] In certain instances, legitimacy rather than legality has been cited as grounds for action, as seen in NATO's bombing of Kosovo in 1999 without any UNSC resolution. Furthermore, some states have neglected to report their use of force to the UNSC.[59] Given the increasing occurrence of drone attacks and the lack of transparency surrounding vital aspects of drone warfare, it is not surprising that numerous questions remain unanswered.

4.2. Use of Unmanned Platforms during Armed Conflict

As previously outlined, deploying a military unmanned platform beyond a state's borders could potentially violate territorial integrity, political independence, or even constitute an act or crime of aggression. Consequently, such actions might instigate an armed conflict, necessitating adherence to the norms outlined in LOAC during the conduct of such hostilities.

54 UNSC, 2001a; UNSC, 2001b; ICJ, 2005, para. 11; Tams, 2009, pp. 359–397.
55 USA, 2014; Australia, 2015; Turkey, 2015.
56 *A plea against the abusive invocation of self-defence as a response to terrorism*, no date.
57 HRC, 2022, pp. 19–20.
58 UNSC, 2015.
59 HRC, 2022, pp. 19–20.

4.2.1. The Unbounded Scope of Armed Conflict

Criticism of the "war on terror" largely stems from its proponents' assertion that it should be classified as a global non-international armed conflict (NIAC), treating terrorist organisations as non-state actors. This classification negates the relevance of geographic boundaries within an armed conflict and lacks a clear endpoint.[60] It implies that a member of such a terrorist group can be targeted or attacked anywhere and at any time. Whereas, according to international law, military operations should be confined to the territories of the aggressors during armed conflicts.[61] Nevertheless, there have been instances where drones were employed by states not directly involved in conflicts or in the territories of states unrelated to ongoing conflicts. These incidents primarily involved targeting specific individuals, such as terrorists, who were located outside the conflict zone and were not engaged in any armed activities at the time. Killing individuals without any attempt to apprehend or offer them the chance to surrender, is inconsistent with international law. The utilisation of drones for these purposes could also result in casualties among bystanders near the target. Any use of UAVs in territories not involved in armed conflict should also be regarded as unlawful.

In this context it is crucial to consider the legal frameworks governing armed conflicts. While actions deemed impermissible during peacetime become lawful under LOAC, it is important to note that IHRL remains applicable. There is a consensus in legal doctrine that these two legal frameworks are complementary. Particularly in NIACs, such as the 'war on terror', IHRL paradigm plays a significant role due to the comparatively limited regulation of NIACs in contrast to international armed conflicts (IACs). The primary distinction lies in law enforcement operations during peacetime, where a suspect is held accountable based on individual guilt and is entitled to a fair trial in a court of law. The use of lethal force in these situations is restricted to cases of self-defence. Any other scenario would be categorised as an extrajudicial execution or murder. However, under the LOAC paradigm, the scope of permissible killings is significantly broader. Such killings do not necessitate judicial review and are not based on individual guilt but rather on the individual's status as designated by the military command and determined through gathered intelligence. Assessments are made beforehand, and only deliberate violations of specific fundamental LOAC principles qualify as international crimes. As a result, standards diverge between these two contexts.[62]

Therefore, the fact that many states have been involved in NIACs for more than 20 years results in substantial tensions, especially concerning the right to life, which, as a human right, also pertains to individuals classified as terrorists.[63]

60 Brooks, 2015.
61 Art. 1(3) AP I.
62 Blum and Heymann, 2013, pp. 69–71.
63 Melzer, 2008a, pp. 91–139; Heyns et al., 2020, pp. 153–189.

4.2.2. Targeting Law

To grasp the transformation of warfare caused by the utilisation of unmanned platforms, it is essential to briefly examine the fundamental principles of targeting employed during armed conflicts.

In armed conflicts, military objectives (lawful targets) include combatants from the enemy state (in both IAC and NIAC) or fighters associated with organised armed groups (in NIAC). Additionally, civilians who directly participate in hostilities can lose their protected status and become targets.[64] Identifying a combatant typically involves them wearing a military uniform with visible insignia and openly carrying a weapon. Under most circumstances, a combatant can be lawfully targeted, irrespective of their activity (such as sleeping, resting, or retreating), except when they are *hors de combat*. The attacking party is not obligated to issue prior warnings, attempt arrest or capture, or minimise casualties among enemy forces.[65]

In the case of fighters in NIACs, the issue of identifying a legitimate military objective becomes considerably more complicated. A status-based classification is crucial again, based on membership of an organised armed group.[66] However, this is challenging due to the dispersed structures of armed organisations, which differ from traditional military entities. Members often do not wear uniforms or openly carry weapons. Additionally, the phenomenon of fighters seamlessly transitioning between combat and civilian roles – referred to as "farmer by day, guerilla by night" or "revolving door" phenomenon – greatly complicates the identification of targets in NIACs.[67]

In all instances, those responsible for planning or authorising an attack must take all feasible measures to verify that the targets are not civilians or civilian objects and do not possess protected status.[68] The burden of proof lies with the attacker to demonstrate incontrovertible evidence, such as an individual's sustained engagement in combat functions within an organised armed group. However, the LOAC does not stipulate exact evidentiary requirements for identifying a civilian as a member of such a group or a person engaged in direct armed activities. Pursuant to Art. 50(1) AP I, when uncertainty arises, the individual must be regarded as a civilian. Therefore, prior to and during the attack, continuous assessment and adaptation based on unfolding circumstances are imperative.

Thus, in principle, civilians are protected under the principle of distinction and cannot be identified as military objectives. However, this does not categorically render the act of killing a civilian impermissible in all circumstances. Two exceptions exist. Firstly, when a civilian directly engages in hostilities, they individually

64 Melzer, 2009, p. 69.
65 Schmitt, 2009, p. 314.
66 Gaggioli, 2018, pp. 901–917.
67 Silvestri, 2020, pp. 410–446.
68 Art. 51 AP I.

forfeit their legally mandated protection. Secondly, civilian casualties may be acceptable if they are incidental, meaning they are not disproportionately high in terms of the anticipated concrete and direct military advantages according to the principle of proportionality. Additionally, the attacking party must take all feasible precautionary measures to minimise incidental harm to civilians according to the principle of precautions. Hence, the conflicting parties are mandated to conduct hostilities in a manner that minimises civilian suffering, loss, and casualties caused by armed conflict.[69]

Drone warfare was envisioned as a solution to reducing civilian casualties; however, its implementation has revealed that precision alone cannot guarantee casualty-free conflict.[70] Moreover, the anticipated precision of drones was not demonstrated in practice.

4.3. Controversial Methods of Warfare

From a legal point of view, the legality of unmanned platforms as a means of warfare, is generally not controversial as there is not a specific ban on them. Rather, the controversy concerns the ways in which unmanned platforms are used since their use is not unrestricted.[71] Key aspects revolve around the direction of the drone during an attack and the manner in which the attack is executed.

An operator of an unmanned platform, holding combatant status as a member of the armed forces, is permitted under LOAC to operate the platform and use lethal force during armed conflicts. However, if the operator is a civilian – for instance, an employee of a private military company or an agent of civilian intelligence services – direct involvement in armed action would contravene the LOAC. Such individuals lack the right to participate directly in armed activities and may face criminal responsibility as a consequence.

The deployment and use of unmanned platforms must adhere to fundamental principles of LOAC and, in cases of NIAC, to all other relevant legal frameworks.[72] Our focus in this chapter will be solely on two methods of their use: targeted killings and signature strikes.

4.3.1. Targeted Killings

The first known public instance of targeted killing beyond a theatre of active war occurred in Yemen in November 2002. A Predator drone, an unmanned and remotely operated platform, was deployed against a car carrying Al-Harethi, suspected

69 Queguiner, 2006, pp. 793–821.
70 Cole, 2018, pp. 793–821.
71 Art. 35 AP I.
72 Heyns et al., 2020, pp. 153–189.

in the U.S.S. Cole bombing, and four others.[73] The Yemen attack had the approval of the Yemeni government, easing some international legal complexities associated with the use of force mentioned earlier.

While no specific international law has defined methods of targeted killing, numerous definitions have been crafted within academic doctrine.[74] Terms synonymous with targeted killings include targeted elimination, targeted self-defence, selective targeting, targeted assassination, extrajudicial killing, and extrajudicial execution. The methods for targeted killings vary, spanning sniper rifle shots or close-range attacks to missile strikes from helicopters, ships, or UAVs. In principle, the following elements of this method of warfare can be distinguished: use of lethal force; intent, deliberateness and planning to cause death (*dolus directus*); elimination of specific, selected persons; no deprivation of liberty; and imputability of the action to a subject of international law (state or non-state).[75] There is no universal consensus on the legality of targeted killings. Advocates often stress its necessity in countering terrorist threats and asymmetric conflicts. However, it blurs and extends the boundaries of applicable laws.[76] Even when assessed under the LOAC, there is a trend in practice to widen the range of permissible targets and conditions for its use. Particularly contentious are the 'double tap' strikes, where an initial attack is followed by another targeting those who offer aid. This often leads to casualties among civilian responders or rescue teams, triggering significant controversy.[77]

The legality of targeted killings hinges on accurately qualifying the situation in which they are used. In cases involving armed conflict, adherence to the LOAC becomes paramount. Hence, it remains imperative to adhere to the delineated targeting principles and conduct a thorough assessment to ascertain the individual's classification as a military target (a combatant or someone directly participating in hostilities). It is equally crucial to ensure that potential collateral damage remains proportionate and that all feasible precautions were implemented beforehand. If targeted killings are contemplated during peacetime, adherence to the law enforcement paradigm – operating under IHRL is essential. In this context, taking someone's life is only justifiable when necessary to protect life, and other alternatives like arrest or non-lethal incapacitation cannot prevent an immediate threat to life. The legality of using lethal force here hinges on meeting the criteria of proportionality and necessity. Proportionality demands that the force employed should be proportional to the level of threat posed by the individual. Necessity mandates minimising the use of force while maintaining a balance between force and the threat at hand.

The use of lethal force through remote attacks from unmanned platforms, even within an appropriate legal framework, presents considerable challenges.[78] In recent

73 Downes, 2004, pp. 277–294.
74 Melzer, 2008b.
75 Ibid., pp. 3–8.
76 Corn, 2019, pp. 246–273.
77 Alexander, 2017, pp. 261–295.
78 IBA, 2017, para. 16.

decades, the United States, Israel, and the United Kingdom have expanded the interpretation of this approach. They have utilised drone attacks in situations where it was more convenient than capturing, trying, or extraditing individuals posing threats to their national interests, often without substantiated justification. This underscores the harmful impact of portraying drone warfare as risk-free, emphasising precision attacks, and promoting the ability to deploy lethal force across the globe.

4.3.2. Signature Strikes

Signature strikes, also known as "crowd killings", were authorised by U.S. President George W. Bush in 2008 to target individuals affiliated with al-Qaeda and Taliban operatives in Pakistan, and later extended by U.S. President Barack Obama to Yemen.[79] Signature strikes are akin to targeted killings but differ in their approach. They can be conducted both within and outside armed conflicts, and therefore, they share the challenges associated with the standards applied in targeted killings.

Signature strikes involve an attack, often carried out by UAV, on a group of individuals sharing a specific characteristic associated with the armed or terrorist activities of an adversary.[80] However, unlike targeted killings, the identity of these individuals is not known beforehand. Instead, targets are chosen based on criteria such as behaviour patterns and personal networks to judge the probability that these individuals qualify as legitimate military targets. Within the framework of the targeting principles previously outlined, the legality of the signature strikes method hinges on an individual's characteristics to classify them as a legitimate target under LOAC, substantiated by clear evidence confirming this characteristic.

However, within the context of LOAC, not all these characteristics or traits are deemed acceptable. These traits can be categorised into three groups based on this perspective.[81] The first group comprises traits that align with LOAC standards, including planning attacks, transporting weapons, planting explosives, or being present at a terrorist organisation's facilities or training camps. The second group encompasses traits that are debatable under the LOAC, such as groups of armed individuals moving towards a combat zone, running training camps for terrorist organisations, participating in training to join a terrorist group, providing support to a terrorist group, or attacking recreational facilities. Finally, the third group pertains to characteristics that are deemed unacceptable under LOAC, including being of draft age in a terrorist-controlled or affected area, associating with terrorists or combatants, or travelling with weapons in trucks within an area controlled by a terrorist organisation.

The primary challenge to the legality of signature strikes arises from the anonymity of targets, making it difficult to uphold the principle of distinction as some of

79 Zenko, 2013, pp. 12–14.
80 Zenko, 2012.
81 Marcinko, 2015.

the targets might be civilians.[82] Cases like the incident in December 2013, which resulted in the death of 12 Yemeni civilians (prompting $1 million in condolence payments from the U.S. government), and the attack in Pakistan that killed 18 workers and injured 22 others, highlight the severe consequences and human toll associated with the use of signature strikes.[83]

4.3.3. The Myth of Precision

The promise of precision in drone warfare, often lauded as a way to limit civilian harm, has faced significant challenges in reality. Several reports of drone strikes that resulted in a significant number of civilian casualties have challenged claims of their precision and efficacy.[84] Operational complexities have resulted in discrepancies between the intended and actual outcomes of drone strikes. Despite advanced technological capabilities, drone operators encounter challenges in accurate target identification and verification within dynamic conflict zones where situations can rapidly change (as described in Chapter 12).

The role of intelligence reports in guiding drone strikes is pivotal. Inaccurate or outdated information about targets, inconsistencies in intelligence assessments, and reliance on remote operators distanced from active conflict zones contribute to misinterpretations and erroneous judgements during strikes.[85] Additionally, the human factor in drone operations introduces the potential for error. Decisions made by operators, often removed from the conflict area, rely on intelligence reports and may lack contextual on-the-ground understanding. These factors collectively highlight why the precision of drone warfare often falls below expectations. Limitations in surveillance technologies and the inherent uncertainties of armed conflicts further complicate matters, challenging the perceived precision of drone strikes and revealing their complexity and fallibility.

---

5. Presenting Responsibility Regimes

This section offers brief insights into the responsibility frameworks applicable to both states (ARSIWA) and individual operators of unmanned platforms (international criminal law). These frameworks are particularly relevant since drone use can result in violations of the prohibition against the use of force, contravene fundamental targeting principles within the LOAC regime, or amount to breaches of IHRL.

82 Buchanan and Keohane, 2015, pp. 22–23.
83 McLeary and DeLuce, 2016.
84 Open Society, 2014; Singh, 2015; Amnesty International, 2020; Khan, 2021.
85 Currier and Maass, 2015.

5.1. State Responsibility

Under international law, a State is accountable for wrongful acts by its agents or actions attributable to it as outlined in the ARSIWA. This type of liability is considered objective, requiring proof of a breach of international legal norms and the imputation of the act to the state (Art. 2). Therefore, actions executed with the use of unmanned platforms operated by a state's armed forces, intelligence agencies, or other state organs are attributable to the state (Art. 4). ARSIWA also delineates various other methods for attributing an act to the state, including actions by entities exercising elements of governmental authority (Art. 5) or entities directed or controlled by the state (Art. 9). In instances where injury is inflicted by such acts, the state is obligated to provide full reparation, including restitution, compensation, and satisfaction (Arts. 34-37). However, a significant challenge arises in collecting evidence, particularly given the lack of transparency from states concerning their drone operations and the actors involved.

An under-explored area pertinent to EU Member States is state responsibility rooted in complicity. The execution of combat drone operations necessitates intelligence sharing and cooperation in terms of lending military bases closer to the target of the attack than those of the drone-sending state or providing logistical and technological support. While most of the practices described in this chapter have been closely associated with the United States, NATO allies and, at the same time, EU members states, have not been entirely inactive in these endeavours. In fact, their support holds substantial significance, as highlighted by Eleonora Branca:

> (…) Germany affords constant support to the U.S. drone operations through the satellite infrastructures of the Ramstein military base. Italy has concluded a series of technical military agreements with the USA allowing the use of the Sigonella air and naval military base to fly U.S. armed drones operating in Libya and in the Mediterranean. A huge amount of data and metadata collected by Netherlands' geo-localisation system are regularly shared with U.S. agencies to be used to identify individuals in counterterrorism operations, especially in Somalia.[86]

There has already been a judicial evaluation of the activities conducted at the Ramstein air base in Germany. The case involves the Bin Ali Jaber family, some of whom were killed in a U.S. drone strike in Yemen in 2012. The remaining family members filed a legal complaint against Germany, in the light of their constitutionally guaranteed right to life, to prevent further attacks linked to the U.S. Ramstein Air Base. In March 2019, the Higher Administrative Court of Münster mandated Germany's responsibility to ensure compliance with international law by the U.S. using the military base. However, in November 2020, the Federal Administrative Court overturned this ruling, asserting that diplomatic efforts by Germany would be

86 Branca, 2022, pp. 253–254.

more suitable than using litigation to discuss potential violations of international law in U.S. drone missions. Although a constitutional court complaint was submitted in 2021, the case is pending a final ruling, illustrating the complex challenges of state responsibility in joint drone operations and the struggles of victims and their families seeking legal recourse.[87]

This leads us to consider the implications of state responsibility under IHRL. A significant challenge arises due to the absence of ratification by all states of specific legal instruments that confer jurisdiction to IHRL courts or bodies. For instance, the United States does not fall under the jurisdiction of the Inter-American Court of Human Rights, nor have they ratified Optional Protocol I to the International Covenant on Civil and Political Rights, which would allow individual complaints to the Human Rights Committee.

The situation varies across European states, particularly those under the jurisdiction of the European Court of Human Rights, which includes all EU Member States. Although the Court has not yet addressed any drone warfare cases, the potential that exists for Member States of the Council of Europe to face scrutiny over drone-related targeted killings, considering previous precedents related to the extraterritorial applicability of the European Convention on Human Rights.[88]

5.2. Operator Responsibility

Debate is lacking in the context of individual responsibility for military robots due to the direct human operation feature (human-in-the-loop), a stark contrast to autonomous systems.[89] The operator's role in a drone's attack aligns with that of a pilot in a manned aircraft, allowing for the application of similar targeting law rules, including potential criminal responsibility for deliberate attacks on civilians and assessments of compensation liability akin to attacks using manned platforms (under Art. 8(2)a(i) and Art. 8 (2)b(i) of the Rome Statute).[90]

It is important to note that individual criminal responsibility is judged on the assessment made before the attack, regardless of its direct impact. Regarding *post-facto* legal responsibility, the decision-makers' access to pertinent information is paramount, particularly in remotely piloted platforms where decisions are contingent upon available data. Individual responsibility evaluations are centred around the reasonableness of decisions, use of potential precautions, attack proportionality, and endeavours to mitigate civilian harm. This underscores the critical role of intelligence reports and operational data, outweighing the significance of the means of warfare employed. The remote nature of the attack significantly amplifies the operator's reliance on this information.

87 ECCHR, 2021.
88 Bodnar and Pacho, 2012, pp. 189–208.
89 Weigend, 2023.
90 Boothby, 2012, pp. 589–594.

In principle, there is potential to assign accountability to operators of unmanned platforms, yet its practical implementation is not straightforward. Most states engaged in drone warfare (such as the United States, Israel, China, India, and Russia) or receiving drone strikes (including Iraq, Libya, Pakistan, Somalia, and Yemen) are not parties to the Rome Statute. Consequently, attempts to prosecute violations of LOAC and IHRL during armed conflicts in national courts have mostly met with limited success. Domestic judges often feel incapable of effectively constraining the state's national security strategies.[91]

6. Common European Drone Strategy

The European discourse on armed drone usage lacks historical depth. While there have been notable advancements, considering the region's aspirations for prosperity, the upholding of the rule of law, and the application of the most rigorous human rights standards, its progress has been slow. The need for a common EU policy regarding drones is essential not only to ensure compliance with the rule of law but also in light of the EU's plans to integrate drone and counter-drone technology into its defence strategies and initiatives.[92]

The most actively involved institution, by a considerable margin, has been the European Parliament (EP). In April 2012, several members of the EP (MEPs) issued a declaration urging the EU to prohibit targeted killings and combat drone operations.[93] In 2013, MEPs organised a briefing on transparency and accountability around U.S. targeted killings, followed by a statement expressing concern about the legal, moral, ethical and IHRL implications of this practice.[94] Additionally, the DG for External Policies of the EU released a study recommending a broad inter-governmental dialogue to seek international consensus on legal standards and constraints for unmanned weapon systems and a binding or non-binding agreement governing drone use.[95]

In February 2014, the Transnational Institute reported on the EU's support for the drone industry.[96] The authors highlighted that drone research and defence subsidies are predominantly shaped by minimally accountable officials and defence corporations, significantly favouring the interests of major defence contractors. They further presented recommendations aimed at mitigating these democratic shortcomings and ensuring the protection of international law and IHRL in this sphere.

91 Casey-Maslen, 2018, pp. 180–193.
92 Borsari and Davis Jr., 2023.
93 *Written declaration on the use of drones for targeted killings*, 2012.
94 Yachot, 2013.
95 Melzer, 2013.
96 Transnational Institute and Statewatch, 2014.

In the same year, the EP adopted Resolution 2014/2567(RSP)[97] condemning illegal drone use; it urged the EU to 'develop an appropriate policy response at both European and global level which upholds human rights and international humanitarian law'. The resolution strongly denounced the unlawful deployment of armed drones, particularly the practice of targeted killings conducted outside declared conflict areas and in violation of established international legal frameworks. It condemned the detrimental impact of such strikes, such as unknown civilian casualties, severe injuries, and traumatic disruptions to civilian lives. It recommended EU Member States to ensure transparency and accountability and refrain from supporting or engaging in extrajudicial targeted killings, including sharing information which could be exploited for illegal targeted killings. When allegations of civilian casualties emerged, states were mandated to conduct prompt, independent investigations and, upon confirmation, publicly assign accountability, penalise those responsible, and facilitate redress, including compensation for affected families. Additionally, the resolution highlighted the urgent need to integrate armed drone production within European and global arms control structures, given regulatory gaps in the rapidly expanding military drone market. The EP removed funding from the EU budget for operations with military or defence implications and urged the European Commission to provide comprehensive information to the EP concerning the use of EU funds allocated to drone development initiatives.

In 2015 the Parliamentary Assembly of the Council of Europe adopted Resolution 2051.[98] The Assembly identified numerous legal concerns arising from ambiguities in compliance with national and international legal frameworks. It stressed that targeted killings should only be used as a last resort when deemed necessary to protect national sovereignty and respect territorial integrity. There was a call upon states to respect the LOAC and IHRL, acknowledging that some states had employed a permissive interpretation of an 'imminent threat'. Transparency in authorisation procedures for targeted killings was deemed crucial, alongside thorough investigations into all casualties caused by drone strikes for accountability and compensation to victims' families. Subsequently, the International Centre for Counter-Terrorism assessed Member States' positions on armed drones, revealing a lack of unified EU positions.[99]

In 2016, the EP reiterated concerns regarding the use of armed drones outside international legal frameworks in Resolution 2016/2662(RSP).[100] In the same year, the European Forum on Armed Drones (a civil society network) launched a Call to Action, urging the EU to articulate clear policies to prevent complicity, ensure transparency, establish accountability and control the proliferation of drones and drone-related technology.[101] In 2017, the Human Rights Subcommittee commissioned

97 EP, 2014.
98 PACE, 2015.
99 Dorsey and Paulussen, 2015.
100 EP, 2016.
101 EFAD, 2016.

a paper on armed drones, outlining the elements for a European-wide policy, legal standards and requirements necessary at the national level to align with the EU's dedication to the rule of law and previous EP resolutions.[102]

Despite extensive deliberations, meetings, and non-binding resolutions, the EU has yet to establish a unified and binding stance on its drone policy. Despite repeated appeals from scientific circles and non-governmental organisations, there has been a dearth of subsequent actions. This situation is partly due to the EU's authority in the Common Security and Defence Policy as delineated in the Chapter 1 and partly to the divergent approaches and differing combat backgrounds of its Member States. However, considering the dynamic security landscape, particularly within the immediate vicinity of the EU, it is essential to develop bolder more ambitious plans and policies for the consolidation of European armies.

7. Conclusions

The multifaceted roles of contemporary military robots – spanning logistics, reconnaissance, and lethal capabilities – highlight the need to delineate their functions and categorise them within a legal framework. These technologies operate in diverse capacities, from aiding humanitarian efforts to engaging in combat, raising critical legal and ethical questions that warrant nuanced examination within the international legal sphere.

The absence of universally recognised definitions for military robots and drones calls for exploring national regulations and policy frameworks, emphasising the need for clear terminology and legal classification. A key distinction in legal and ethical discourse is between autonomous military robots and those involving human oversight. The demarcation between remotely controlled systems and autonomous entities underscores the significance of human control over these technologies, an important concept in discussions around compliance with international law (including the use of force, LOAC and IHRL) and the attribution of responsibility for their actions.

The intricate relationship between humanitarian considerations and state interests exposes the diverse motivations underlying weapon regulations. Military robots are difficult to regulate, owing to their unique attributes, necessitating an examination of broad regulations to navigate the complex legal landscape governing their development and deployment. This analysis also exposes the absence of specific international norms defining these technologies, highlighting the pivotal role of doctrine in shaping discussions. Classified as weapon platforms, military robots pose a distinct challenge, demanding scrutiny of their classification as a means of warfare but, critically, the legality of their method of use.

102 Dorsey and Bonacquisti, 2017.

Despite fundamental principles of LOAC being embedded in international law, such as the legal review under art. 36 AP I, the inconsistent practice of these reviews raises concerns about their effectiveness in regulating disruptive technologies like military robots. The challenge lies in sourcing diverse expertise to evaluate these technologies and developing unified global standards, which are currently lacking. With divergent interpretations of international legal norms among states, a unified framework becomes crucial to ensure ethical, lawful, and accountable development and deployment of modern weaponry. Within the EU, Member States vary in their approaches to reviewing new weapons, highlighting the pressing need for harmonised, transparent, and enforced standards, at least at the regional level.

The proliferation of UAVs, particularly in the "war on terror", complicates established doctrines, particularly the notions of pre-emptive self-defence and response to non-state actor attacks, sparking contentious debates on imminency, necessity, and proportionality within the use of force framework. Deploying military unmanned platforms outside a state's borders raises substantial legal concerns, potentially violating territorial integrity and sovereignty.

Using unmanned platforms to apply lethal force in targeted killings and signature strikes causes legal ambiguity. While the targeting principles under the LOAC govern legitimate military objectives, the difficulty of distinguishing between combatants and civilians in NIACs raises crucial concerns. This challenge often contradicts the perceived precision of drone strikes, amplifies concerns about collateral damage, and raises questions about the validity and ethical justification of using these operations.

The attribution of state responsibility for actions executed through unmanned platforms is a challenging endeavour. The crux of the matter lies in the collection of evidence, which is significantly impeded by the lack of transparency exhibited by states. This lack of openness hampers the process of seeking reparation for injuries or harm inflicted by these actions. Moreover, operators engaged in drone operations, similar to pilots in manned aircraft, may bear individual criminal responsibility. However, the enforcement of this responsibility is challenging due to the limited avenues available for prosecution at both international and national levels. This complexity is further exacerbated when the states involved are not signatories to key legal frameworks governing armed conflict and human rights, creating an intricate legal landscape for accountability.

The EU's discourse on using armed drones has seen notable advancements but remains limited, considering its commitment to upholding the rule of law and rigorous human rights standards. Establishing a common EU policy on drones becomes imperative in light of the region's integration of drone technology into defence strategies and the lack of transparency in operations. Despite extensive discussions and non-binding resolutions, the EU has not achieved a unified, binding policy on drone use due to divergent Member State'a approaches, differing experiences of combat, and limitations within the CSDP. The lack of actions following repeated appeals from scientific and non-governmental circles underscores the challenges of consolidating a coherent EU-wide approach to drones.

References

Additional Protocol (I) to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts (1977) Geneva, 8 June 1977.

Abbott, K. (2014) 'A brief overview of legal interoperability challenges for NATO arising from the interrelationship between IHL and IHRL in light of the European Convention on Human Rights', *International Review of the Red Cross*, 96(893), pp. 107–137; https://doi.org/10.1017/S1816383115000338.

Acquaviva, G. (2023) 'Crimes without Humanity? Artificial Intelligence, Meaningful Human Control, and International Criminal Law', *Journal of International Criminal Justice*, 21(5), pp. 981–1004; https://doi.org/10.1093/jicj/mqad024.

Alexander, S. (2017) 'Double-Tap Warfare: Should President Obama Be Investigated for War Crimes?', *Florida Law Review*, 69(1), pp. 261–295.

Amnesty International (2020) 'The US military is ramping up its secret air war in Somalia, with a deadly impact for civilians on the ground', 1 April 2020. [Online]. Available at: https://www.amnesty.org/en/latest/news/2020/04/somalia-zero-accountability-as-civilian-deaths-mount-from-us-air-strikes/ (Accessed: 15 January 2024).

Anderson, S.R. (2020) 'Did the President Have the Domestic Legal Authority to Kill Qassem Soleimani?', *Lawfare*, 3 January 2020. [Online]. Available at: https://www.lawfaremedia.org/article/did-president-have-domestic-legal-authority-kill-qassem-soleimani/ (Accessed: 15 January 2024).

Argentina (2019) *Questionnaire on the Legal Review Mechanisms of New Weapons, Means and Methods of Warfare*. CCW/GGE.1/2019/WP.6 [Online]. Available at: https://perma.cc/7UVP-9YFV/ (Accessed: 15 January 2024).

Articles on Responsibility of States for Internationally Wrongful Acts (2001) United Nations, A/56/10.

Australia (2015) *Letter dated 9 September 2015 from the Permanent Representative of Australia to the United Nations addressed to the President of the Security Council*. S/2015/693.

Blum, G., Heymann, P.B. (2013) *Laws, outlaws, and terrorists: lessons from the war on terrorism*. (ed.) Cambridge, MA.: MIT Press.

Bober, W.J. (2015) 'Czy korzystanie z bojowych bezzałogowych pojazdów latających jest moralnie problematyczne?' [Is military use of armed drones morally problematic?] in Kowalewski, J., Kowalczewska, K. (eds.) *Systemy dronów bojowych: analiza problemów i odpowiedź społeczeństwa obywatelskiego* [Combat drones systems: problem analysis and civil society answer]. Warsaw: Wydawnictwo Naukowe Scholar, pp. 32–47. [Online]. Available at: https://www.legal-tools.org/doc/90ffec/ (Accessed: 15 January 2024).

Bodnar, A., Pacho, I. (2012) 'Targeted Killings (Drone strikes) and the European Convention on Human Rights', *Polish Yearbook of International Law*, 2012/32, pp. 189–208.

Boothby, W. (2012) 'Some legal challenges posed by remote attack', *International Review of the Red Cross*, 94(886), pp. 579–595; https://doi.org/10.1017/S1816383112000719.

Borsari, F., Davis, Jr., G.B. (2023) 'Drones are changing warfare – the EU needs to catch up', *Politico*, 26 December 2023. [Online]. Available at: https://www.politico.eu/article/drones-are-changing-warfare-the-eu-needs-to-catch-up-ukraine-gaza-conflicts/ (Accessed: 15 January 2024).

Branca, E. (2022) 'Complicity of States in Partnered Drone Operations', *Journal of Conflict and Security Law*, 27(2), pp. 253–278; https://doi.org/10.1093/jcsl/krac011.

Brooks, R. (2014) 'Drones and the International Rule of Law', *Ethics & International Affairs*, 28(1), pp. 83–103; https://doi.org/10.1017/S0892679414000070.

Brooks, R. (2015) 'There's No Such Thing as Peacetime', *Foreign Policy*, 13 March 2015. [Online]. Available at: https://foreignpolicy.com/2015/03/13/theres-no-such-thing-as-peacetime-forever-war-terror-civil-liberties/ (Accessed: 15 January 2024).

Buchanan, A., Keohane, R.O. (2015) 'Toward a Drone Accountability Regime', *Ethics & International Affairs,* 29(1), pp. 15–37; https://doi.org/10.1017/S0892679414000732.

Capek, K. (1920) *R. U. R.: Rossum's Universal Robots*. Prague: Aventinum.

Casey-Maslen, S. (2018) 'Unmanned Weapons Systems and the Right to Life' in Casey-Maslen, S., Homayounnejad, M., Stauffer, H., Weizmann, N. (eds.) *Drones and Other Unmanned Weapons Systems under International Law.* Leiden: Brill/Nijhoff, pp. 158–194; https://doi.org/10.1163/9789004363267_008.

The Charter of the United Nations (1945) 1 UNTS XVI.

Cole, C. (2018) 'Thinking war is bloodless is a mistake. Talking drones and remote war with Air Marshall Bagwell', *Dronewars*, 8 January 2018. [Online]. Available at: https://dronewars.net/2018/01/08/thinking-war-is-bloodless-is-a-mistake-talking-drones-and-remote-war-with-air-marshall-bagwell/ (Accessed: 15 January 2024).

Copeland, D., Liivoja, R., Sanders, L. (2023) 'The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems', *Journal of Conflict and Security Law*, 28(2), pp. 285–316; https://doi.org/10.1093/jcsl/krac035.

Corn, G. (2019) 'Drone Warfare and the Erosion of Traditional Limits on War Powers' in Ohlin, J.D. (ed.) *Research Handbook on Remote Warfare.* Cheltenham: Edward Elgar Publishing, pp. 246–273.

Coyne, C., Hall, A. (2018) 'The Drone Paradox. Fighting Terrorism with Mechanized Terror', *The Independent Review*, 23(1), pp. 51–67.

Currier, C., Maass, P. (2015) 'Firing Blind: Critical intelligence failures and the limits of drone technology', *The Intercept*, 15 October 2015. [Online]. Available at: https://theintercept.com/drone-papers/firing-blind/ (Accessed: 15 January 2024).

Development, Concepts and Doctrine Centre (2022) 'Joint Doctrine Publication 0-30. UK Air Power', *UK Ministry of Defence*, September 2022. [Online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1116428/UK_Air_Power_JDP_0_30.pdf (Accessed: 15 January 2024).

Dorsey, J., Bonacquisti, G. (2017) *Towards an EU common position on the use of armed drones.* EP/EXPO/B/COMMITTEE/FWC/2013-08/Lot8/11. DG for External Policies of the Union. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/578032/EXPO_STU(2017)578032_EN.pdf (Accessed: 15 January 2024).

Dorsey, J., Paulussen, C. (2015) *Towards a European Position on Armed Drones and Targeted Killing: Surveying EU Counterterrorism Perspectives*. The Hague: The International Centre for Counter-Terrorism. [Online]. Available at: https://www.icct.nl/sites/default/files/import/publication/ICCT-Dorsey-Paulussen-Towards-A-European-Position-On-Armed-Drones-And-Targeted-Killing-Surveying-EU-Counterterrorism-Perspectives.pdf (Accessed: 15 January 2024).

Downes, C. (2004) '"Targeted Killings" in an Age of Terror: The Legality of the Yemen Strike', *Journal of Conflict & Security Law*, 9(2), pp. 277–294; https://doi.org/10.1093/jcsl/9.2.277.

DroneWars.net (2023) *Who has Armed Drones?.* [Online]. Available at: https://dronewars.net/who-has-armed-drones/ (Accessed: 15 January 2024).

European Center for Constitutional and Human Rights (2021) 'Ramstein before the constitutional court: Germany's responsibility in US drone strikes in Yemen', 23 March 2021. [Online]. Available at: https://www.ecchr.eu/en/press-release/ramstein-constitutional-court/ (Accessed: 15 January 2024).

EFAD (2016) *Call to Action.* [Online]. Available at: https://www.efadrones.org/call-to-action/ (Accessed: 15 January 2024).

European Parliament (2014) *European Parliament resolution of 27 February 2014 on the use of armed drones (2014/2567(RSP)).*

European Parliament (2016) *European Parliament resolution of 28 April 2016 on attacks on hospitals and schools as violations of international humanitarian law (2016/2662(RSP)).*

Farrant, J., Ford, C. (2017) 'Autonomous Weapons and Weapon Reviews: The UK Second International Weapon Review Forum', *International Law Studies*, 93(1), pp. 389–422.

Gaggioli, G. (2018) 'Targeting Individuals Belonging to an Armed Group', *Vanderbilt Journal of Transnational Law,* 51(3), pp. 901–917.

The General Treaty for Renunciation of War as an Instrument of National Policy (1928) Paris, 27 August 1928.

Hagger, M., McCormack, T. (2012) 'Regulating the Use of Unmanned Combat Vehicles: Are General Principles of International Humanitarian Law Sufficient?'*, Journal of Law, Information and Science*, 21(1), pp. 1–26.

Heyns, C., Akande, D., Hill-Cawthorne, L., Chengeta, T. (2020) 'The Right to Life and the International Law Framework Regulating the Use of Armed Drones' in Akande, D., Kuosmanen, J., McDermott, H., Roser, D. (eds.) *Human Rights and 21st Century Challenges*. Oxford: Oxford University Press, pp. 153–189; https://doi.org/10.1093/oso/9780198824770.003.0008.

Human Rights Council (2010) 'Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston: Addendum – Study on targeted killings', A/HRC/14/24/Add.6.

Human Rights Council (2020) 'Use of armed drones for targeted killings. Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions', A/HRC/44/38.

Human Rights Council (2022) 'Position of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism on the use of armed drones in the context of counter-terrorism'. [Online]. Available at: https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/activities/20230103-Position-Paper-Use-Armed-Drones.pdf (Accessed: 15 January 2024).

Human Rights Watch (2012) 'Losing humanity: the case against killer robots', November 2012. [Online]. Available at: https://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf (Accessed: 15 January 2024).

Human Rights Watch (2015) 'Mind the Gap: The Lack of Accountability for Killer Robots', 9 April 2015. [Online]. Available at: https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots (Accessed: 15 January 2024).

International Bar Association (2017) 'International Bar Association's Human Rights Institute Council Resolution on the use of drones for the delivery of lethal weapons', 25 May. [Online]. Available at: https://www.ibanet.org/document?id=4C101874-160A-45EE-A69A-2FBEC026295E (Accessed: 15 January 2024).

International Committee of the Red Cross (2006) 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977', *International Review of the Red Cross*, 88(864), pp. 931–956.

International Court of Justice (2005) *Armed Activities on the Territory of the Congo. Separate Opinion of Judge Simma*. [Online]. Available at: https://www.icj-cij.org/sites/default/files/case-related/116/116-20051219-JUD-01-05-EN.pdf (Accessed: 15 January 2024).

International Organization for Standardization (2012) 'About ISO/TC 299 Robotics'. [Online]. Available at: https://committee.iso.org/home/tc299 (Accessed: 15 January 2024).

Jevglevskaja, N. (2018) 'Weapons Review Obligation under Customary International Law', *International Law Studies*, 2018/94, pp. 186–221.

Jevglevskaja, N., Liivoja, R. (no date) *National Practice on the Legal Review of Weapons, Means and Methods of Warfare*. [Online]. Available at: https://apils.org/legal-review/ (Accessed: 15 January 2024).

Kate-Devitt, S. (2018) 'Trustworthiness of Autonomous Systems' in Abbass, H.A., Scholz, J., Reid, D. (eds.) *Foundations of Trusted Autonomy*. Cham: Springer International Publishing, pp. 161–184; https://doi.org/10.1007/978-3-319-64816-3_9.

Khan, A. (2021) 'Hidden Pentagon Records Reveal Patterns of Failure in Deadly Airstrikes', *The New York Times*, 18 December 2021. [Online]. Available at: https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian-deaths.html (Accessed: 15 January 2024).

Lubold, G., Harris, S. (2017) 'Trump Broadens CIA Powers, Allows Deadly Drone Strikes', *Wall Street Journal*, 13 March 2017. [Online]. Available at: https://www.wsj.com/articles/trump-gave-cia-power-to-launch-drone-strikes-1489444374 (Accessed: 15 January 2024).

Marcinko, M. (2015) *Jak rozwój techniki wojskowej wpływa na sposób prowadzenia współczesnych wojen: targeted killings, signature strikes, drone warfare* [How developments in military technology are influencing the way modern wars are fought: targeted killings, signature strikes, drone warfare]. Polish Red Cross.

McLeary, P., DeLuce, D. (2016) 'Obama's Most Dangerous Drone Tactic Is Here to Stay', *Foreign Policy*, 5 April 2016. [Online]. Available at: https://foreignpolicy.com/2016/04/05/obamas-most-dangerous-drone-tactic-is-here-to-stay/ (Accessed: 15 January 2024).

Melzer, N. (2008a) 'Law Enforcement and the Conventional Human Right to Life' in Melzer, N. (ed.) *Targeted Killing in International Law*. Oxford: Oxford University Press, pp. 91–139; https://doi.org/10.1093/acprof:oso/9780199533169.003.0006.

Melzer, N. (2008b) *Targeted Killing in International Law*. 1st edn. Oxford: Oxford University Press; https://doi.org/10.1093/acprof:oso/9780199533169.001.0001.

Melzer, N. (2009) *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law*. Geneva: International Committee of the Red Cross. [Online]. Available at: https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf (Accessed: 15 January 2024).

Melzer, N. (2013) 'Human rights implications of the usage of drones and unmanned robots in warfare', *Directorate-General for External Policies, Policy Department*, EXPO/B/DROI/2012/12. [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPO-DROI_ET(2013)410220_EN.pdf (Accessed: 15 January 2024).

Meron, T. (2000) 'The Martens Clause, Principles of Humanity, and Dictates of Public Conscience', *American Journal of International Law*, 94(1), pp. 78–89; https://doi.org/10.2307/2555232.

Moyes, R. (2016) 'Key elements of meaningful human control', *Background Paper*, Geneva, 11-15 April 2016. [Online]. Available at: https://article36.org/wp-content/uploads/2016/04/MHC-2016-FINAL.pdf (Accessed: 15 January 2024).

NATO (2021) 'Nato Glossary of Terms and Definitions', AAP-06, 15 December 2021. [Online]. Available at: https://standards.globalspec.com/std/14486494/aap-06 (Accessed: 15 January 2024).

NewAmercia.org (no date) *Who Has What: Countries with Armed Drones*. [Online]. Available at: https://www.newamerica.org/future-security/reports/world-drones/who-has-what-countries-with-armed-drones (Accessed: 15 January 2024).

Olson, P.M. (2013) 'A NATO perspective on applicability and application of IHL to multinational forces', *International Review of the Red Cross*, 95(891–892), pp. 653–657; https://doi.org/10.1017/S1816383114000150.

Open Society (2014) 'After the Dead Are Counted: U.S. and Pakistani Responsibilities to Victims of Drone Strikes', November 2014. [Online]. Available at: https://www.opensocietyfoundations.org/publications/after-dead-are-counted-us-and-pakistani-responsibilities-victims-drone-strikes (Accessed: 15 January 2024).

PACE (2015) *Drones and targeted killings: the need to uphold human rights and international law*.

A plea against the abusive invocation of self-defence as a response to terrorism (no date). [Online]. Available at: https://cdi.ulb.ac.be/wp-content/uploads/2016/06/A-plea-against-the-abusive-invocation-of-self-defence.pdf/ (Accessed: 15 January 2024).

The Program on Humanitarian Policy and Conflict Research (2013) *HPCR Manual on international law applicable to air and missile warfare*. New York, NY: Cambridge University Press.

Queguiner, J.-F. (2006) 'Precautions under the law governing the conduct of hostilities', *International Review of the Red Cross*, 88(864), pp. 793–821; https://doi.org/10.1017/S1816383107000872.

Richards, N., Smart, W. (2016) 'How should the law think about robots?' in Calo M.R., Michael Froomkin, A., Kerr, I. (eds.) *Robot law*. Cheltenham, UK: Edward Elgar Publishing, pp. 3–22; https://doi.org/10.4337/9781783476732.00007.

Rome Statute of the International Criminal Court (1998) ISBN No. 92-9227-227-6, The Hague: International Criminal Court.

Sandoz, Y., Swiniarski, C., Zimmermann, B. (eds.) (1987) *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: Martinus Nijhoff Publishers.

Santoni De Sio, F., Van Den Hoven, J. (2018) 'Meaningful Human Control over Autonomous Systems: A Philosophical Account', *Frontiers in Robotics and AI*, 2018/5, p. 15. https://doi.org/10.3389/frobt.2018.00015.

Schmitt, M. (2009) 'Targeting and International Humanitarian Law in Afghanistan', *International Law Studies*, 2009/85, pp. 307–339.

Silvestri, A. (2020) 'The "Revolving Door" of Direct Participation in Hostilities: A Way Forward?', *Journal of International Humanitarian Legal Studies*, 11(2), pp. 410–446; https://doi.org/10.1163/18781527-bja10022.

Singh, A. (2015*) Death by drone. Civilian harm caused by U.S. targeted killing in Yemen*. New York, NY: Open Society Foundations [Online]. Available at: https://www.justiceinitiative.org/uploads/1284eb37-f380-4400-9242-936a15e4de6c/death-drones-report-eng-20150413.pdf (Accessed: 15 January 2024).

Sterio, M. (2018) 'Lethal Use of Drones: When the Executive Is the Judge, Jury, and Executioner', *The Independent Review*, 23(1), pp. 35–50.

Tams, C. (2009) 'The Use of Force against Terrorists', *European Journal of International Law*, 20(2), pp. 359–397; https://doi.org/doi: 10.1093/ejil/chp031.

Hayes, B., Jones, Ch., Toepfer, E. (2014) *Eurodrones Inc*. [Online]. Available at: https://www.tni.org/files/download/011453_tni_eurodrones_inc_br_3e.pdf (Accessed: 15 January 2024).

Turkey (2015) *Letter dated 24 July 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Turkey to the United Nations addressed to the President of the Security Council*. S/2015/563.

United Nations General Assembly (1974) *Definition of Aggresion*, A/RES/3314(XXIX).

United Nation Security Council (2001a) *Threats to international peace and security caused by terrorist acts* S/RES/1368(2001).

United Nation Security Council (2001b) *Resolution 1373 (2001)*, S/RES/1373.

United Nation Security Council (2015) *Resolution 2249 (2015)*, S/RES/2249.

United States of America (2014) *Letter dated 23 September 2014 from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General.* S/2014/695.

Walsh, J.I., Schulzke, M. (2015) *The Ethics of Drone Strikes: Does Reducing the Cost of Conflict Encourage War?*. United States Army War College Press. [Online]. Available at: https://apps.dtic.mil/sti/tr/pdf/ADA621793.pdf (Accessed: 15 January 2024).

Walsh, J.I. (2015) 'Precision Weapons, Civilian Casualties, and Support for the Use of Force', *Political Psychology*, 36(5), pp. 507–523; https://doi.org/10.1111/pops.12175.

Watts, S. (2015) 'Regulation-Tolerant Weapons, Regulation-Resistant Weapons and the Law of War', *International Law Studies,* 91(1), pp. 540–621.

Weigend, T. (2023) 'Convicting Autonomous Weapons?: Criminal Responsibility of and for AWS under International Law', *Journal of International Criminal Justice*, p. mqad037; https://doi.org/10.1093/jicj/mqad037.

White House (2013) 'Remarks by the President at the National Defense University', *Office of the Press* Secretary, 23 May. [Online]. Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/remarks-president-national-defense-university (Accessed: 15 January 2024).

Written declaration on the use of drones for targeted killings (2012) 16 January 2012, 0002/2012. [Online]. Available at: https://www.europarl.europa.eu/doceo/document/DCL-7-2012-0002_EN.pdf?redirect (Accessed: 15 January 2024).

Yachot, N. (2013) 'European Parliament Members Speak Out Against U.S. Targeted Killing Program', *American Civil Liberties Union*, 7 March 2013. [Online]. Available at: https://www.aclu.org/news/national-security/european-parliament-members-speak-out-against-us-targeted (Accessed: 15 January 2024).

Zenko, M. (2012) 'Targeted Killings and Signature Strikes', *Council on Foreign Relations*, 16 July 2012. [Online]. Available at: https://www.cfr.org/blog/targeted-killings-and-signature-strikes (Accessed: 15 January 2024).

Zenko, M. (2013) 'Reforming U.S. Drone Strike Policies', *Council on Foreign Relations*, Council Special Report No. 65. [Online]. Available at: https://cdn.cfr.org/sites/default/files/pdf/2012/12/Drones_CSR65.pdf (Accessed: 15 January 2024).

IV.5

CYBER WARFARE

Chapter 14

Cyberattacks/Incidents and Responding to Them

Barbara Kaczmarczyk

Abstract

The 21st century has brought forth the digital age. In the past, various types of activities and services could only be performed in the real world, and could be understood without computers. Currently, digital development has rendered possible the performance of numerous, if not almost all, everyday activities online. Services such as online shopping, booking trips, and opening bank accounts are also currently more financially profitable than traditional methods, as well as less time-consuming. Importantly, it is also possible to conduct elections and educational or product promotional campaigns via the Internet in today's digital world, and to conduct fast, free searches for various different pieces of information and large datasets. Digitalisation has undoubtedly contributed to the development of many areas of human life, groups, and institutions. The development of civilization and the digital world also led to the rise of various mechanisms, such as incidents or cyberattacks, that can disrupt these processes. Some of the reasons underlying incidents or cyberattacks, which are highly varied, include achieving quick financial success and destabilising the functioning of specific groups or organisations. Therefore, it is very important to recognise how incidents or cyberattacks work and how to prepare for them, prevent them, and if they occur, how to respond to them. It is also important to restore the status to that before the occurrence of the incidents or the cyberattack.
Research methodology: The article was developed based on Polish and international literature on the subject of security and cybersecurity, as well as Internet sources. During the research process, interviews with cybersecurity experts were conducted.

Keywords: cyber incident, cyberattack, cybersecurity, cyber space, cyber defence

Barbara Kaczmarczyk (2024) 'Cyberattacks/Incidents and Responding to Them'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 619–661. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_14

1. Introduction

The 1940s saw the beginning of work on computers at the University of Pennsylvania, where Eckert and Muachly started building the first computer. They created the Electronic Numerical Integrator and Computer,[1] also known as ENIAC, a machine with an area of over 160 m^2 and a weight of 27 tons, which was considered the first computer in the world. Scientific developments continued, and in the 1970s and 1980s, the first negative computer-related event occurred, caused by the destabilisation of the functioning of the computer network. These phenomena are related to the topics of cyberspace (cyberspace) and digital environment, which also happen to be the places where cybersecurity works.

When considering incidents and cyberattacks, one should start by identifying what they are and in what space they operate.

An incident should be understood as an event that has or may have an adverse impact on cybersecurity.[2] It occurs in cyberspace, which is why we can talk about a security incident, which means that it is an event that may violate the confidentiality, integrity or availability of information and resources of an organization. In the context of security, an incident refers to a sudden and unexpected event that may have negative consequences for people, property, data or infrastructure. Security incidents can concern various aspects of an organization, including personal data, hardware or software.[3] In relation to the term cyberattacks, one definition of cyberattack[4] describes it as an intentional act intended to alter, disrupt, deceive, degrade, or destroy computer systems, networks, and programs serving resident work or enabling the use of these systems or networks. Cyberattacks are hence threats related to the use of computer networks and various criminal activities, such as obtaining material and intangible benefits. This definition can be supplemented by the purpose of such actions, which is often to disrupt security. These attacks are conducted using various methods, such as phishing, malware, ransomware, and distributed denial of service (DDoS) attacks.[5] They are carried out in an unauthorised manner with the purpose of stealing data, or even disrupt or damaging someone's reputation.

Vulnerabilities in systems and software errors facilitate attacks. They are dangerous primarily for national security, but can also be a threat for all other important sectors of society.[6] Cyberattacks[7] occur in cyberspace, defined as the space in which all activities based on information technology, electronic communication, and data processing occur. It is a place where information is exchanged using

1 Celebrating Penn Engineering History: ENIAC, *no date*.
2 Art. 2 ust. 5 Act of 5 July 2018 on the national cybersecurity system; Dz.U. 2018, poz.1560.
3 Based on *Incydent bezpieczeństwa informacji – kiedy następuje?* [Information security incident – when does it occur and what to do?], 2024.
4 Czekaj, 2020. Based on Wasiuta and Klepik, 2019, pp. 175–179.
5 More: European Court of Auditors, 2019.
6 Based on Wasiuta and Klepk, 2019.
7 Based on *Cyberatak* [Cyber attack], 2020.

networks, systems, and the Internet. Accompanying the land, sea, air, and space environments, cyberspace has also been recognised and classified as a new environment category where warfare can be carried out.[8] Cyberspace[9] and the threats emerging in it, which are developing at a rapid pace, have led people to start to think, discuss, and consequently create cybersecurity measures.[10] Related undertakings have, nonetheless, become difficult because everything that occurs in a given environment can be both safe and dangerous. For this reason, risk management strategies, crisis management systems, critical infrastructure management systems, and technical security measures have been developed and implemented. The essence of these measures is to ensure the integrity, confidentiality, and availability of data in the cyberspace, as well as its protection against various types of cyber incidents. Accordingly, information security effectiveness has become increasingly important, to the point that it is now, in the era of digitalisation, crucial to information protection. In this context, information environment analysis (also known as IEA) is very important, comprising data identification, analysis, verification, and interpretation in a changing environment. This showcases that determining the sources of information and their credibility are important undertakings when navigating the cyberspace.

This is especially important if we consider that many decisions can be made based on the acquired information, and that these decisions always accompany consequences. For example, in areas in which information use can translate to either life or death situations, such as in security management, crisis management, and warfare, the cruciality of reliable information is indisputable. This is because information reliability in these settings, which tend to be under constant time pressure, translate into right decisions, saving lives, securing health, and upholding property. In contrast, a lack of information credibility might have irreversible negative effects, such as country destabilisation.[11]

Following this rationale, discussions surrounding the information environment should also touch upon cybersecurity. The importance and power of information should be thoroughly emphasised in the modern world, where information is ubiquitous and of great importance in all areas of life. There is also the recent advent of the Internet, which enabled information to spread easily, instantly, and unlimitedly. In general, information should be treated as an abstract object that can be saved in an encoded format (on information media), transmitted, processed using computer programs, and used to control devices. It is also important to distinguish, in information environments, between an information system and an information technology (IT) system. Information systems feature multilevel structures designed to process input and output information, whereas IT systems refer to the separate,

8 Marczyk, 2018, pp. 59–60; based on European Union Agency for Cybersecurity, 2021.
9 Based on Wasiuta and Klepk, 2019.
10 Cendrowski, 2020.
11 Based on *Analiza ryzyka w obszarze cyberbezpieczeństwa – jakie jest jej znaczenie?* [Risk analysis in the area of cybersecurity – what is its importance?], no date.

computerised parts of information systems, including computers, data storage devices, software, human resources, and knowledge bases.

These descriptions also bring to the fore the concept of IT system security, referring to all activities focused on securing data stored on devices and disabling their accessibility to unauthorised people. Moreover, the concept of information security is defined as 'the desired level of protection of necessary information resources, technologies for their creation and use, as well as the rights of business entities', meaning that such security focuses on assuring that the information system will uphold its stable functioning under all conditions, both at the international and national levels. Each system processes specific types of data, and the main threats to information systems include human errors, crises (i.e. accordingly, additional information systems should be located remotely to reduce the risk of failure), equipment damage and failures (i.e. which can be dealt with by creating backup copies), and planned threats (i.e. avoiding such threats requires the installation of antivirus programs).

Network security depends on several factors, which are generally illustrated in the Cyberspace Security Model across its three pillars, which are[12] (a) confidentiality, which refers to data confidentiality and privacy; (b) inviolability/integrity, which refers to data integrity and system integrity; (c) availability.

2. Evolution of cyberattacks and incidents – case studies

Over the years, there have been many cyberattacks and incidents targeting different systems. The first appeared in 1971 and was a test, but cyberattacks began to take different forms and become increasingly aggressive over time, focusing on specific intentions. They evolved annually until they eventually became war weapons. This section explores the development of cyberattacks from their very beginning, key cases, as well as procedures to be followed in the event of this type of attack. Regarding procedures, it is important to emphasise that they should be aimed at preparing for cyberattacks through planned actions, preventing them, and restoring the status before attack occurrence. These procedures must also be developed considering the individual needs of specific entities, along with the guidelines and recommendations of security entities.

There is a wide catalogue of cyberattacks that occurred in the beginnings of this phenomenon, the most popular and important of which include the following: (a) the "Creeper" virus, (b) the Elk Cloner virus for Apple II, (c) PC virus, (d) Morris virus, (e) the attack on Microsoft, (f) DDoS attacks during the Y2K Crisis, (g) the

12 *Triada CIA – Podstawowe Spojrzenie Na Bezpieczeństwo Informacji* [The CIA Triad – A Basic View of Information Security], 2021.

cyberattacks on Estonia, (h) the Stuxnet attack, (i) the ransomware attack on Target, (j) the WannaCry attack, (k) the SolarWinds attack.

The "Creeper" virus appeared in 1971[13] in the United States of America, and was the first virus to appear on the Internet. Its creator was Bobs Thomas, an employee of a technology company. Its appearance initiated discussions on malware and cybersecurity, and it is because of this virus that terms such as virus, malware, and cybersecurity are now used worldwide. The virus infected computers with the TENEX operating system and that used the ARPANET network. This network was built by the United States Department of Defense as a research experiment, and marked the beginning of the modern Internet. The "Creeper" should be treated as a "program" virus and its activity was not aimed at harming, but only at spreading in the ARPANET network. Its appearance in the operating system was marked by the display of the message 'I'm the creeper, catch me if you can!' The infections with the "Creeper" then lead to the creation of the "Reaper" program, created to remove this virus from infected systems. This incident became the basis for work on computer security standards; importantly, at that time, there were not many options available for protecting a system against this type of virus, and awareness of this phenomenon was only starting to arise.

Regarding the management of this virus in case it infects a system, the following steps should be followed: (a) isolate the system from others to prevent its spread, (b) analyse the behaviour of the virus to develop effective removal tools and strategies, and (c) manually remove it from the infected systems. Importantly, the creation of this virus gave rise to the "Reaper" program, which in turn led to discussions about viruses, malware, and cybersecurity. This entails that the "Creeper" virus gave stakeholders impetus to start developing and discussing Internet security rules, the first antivirus tools, and operating system security and updating.

The Elk Cloner virus appeared in 1982[14] in the United States of America and was one of the first computer viruses to appear on Apple II computers. Its creator, Rich Skrenta, was a teenage student at the University of Illinois. The goal with the Elk Cloner virus was not to create danger but to raise awareness about viruses and their ability to spread on computers. This virus did not cause any loss or damage, and but rather displayed a humorous message warning about its capabilities when launched.

Regarding the management of this virus in case it infects a system, the following steps should be followed: (a) isolate the system isolation (i.e. floppy disks should not be used on other computers); (b) scan floppy disks; (c) create and use backups; (d) increase user awareness (i.e. educate the public about IT security and applying rules for using floppy disks of unknown origin); (e) update software.

13 Encyclopedia by Kaspersky, no date; Thomson and Nichols, 2009.

14 Sarkar, 2023; Thomson and Nichols, 2009; *Elk Cloner. La cápsula del tiempo* [Elk Cloner. The Time Capsule], 2009.

The first PC virus appeared back in 1986,[15] Which was also a breakthrough year for viruses. The "PC" (Brain) virus was one of the most harmful ones, and its attacks were focused on the MS-DOS system, which was still used on PCs and mostly in business environments. It was created by the Pakistani programmers Basita and Amjad Farooga. The actions of this virus were much more advanced than those of the two aforementioned viruses, as it infected sectors of hard drives and led the computer to boot with the infected code instead of the original boot. That is, the virus took over control over the booting process, launching the Brain program simultaneously to the original boot every time a computer was booted. Despite the complexity of the operation of the virus, it is did not incorporate any type of intent, such as stealing data or information, but rather was experimental. The virus creators actually included their data, such as telephone number, address, and information about the infection, in the computer code. Despite the lack of malicious intent, this still configured the first malware threat in the world, and it is important to note that computers at the time of the malware's creation were relatively small in scale.

Regarding the management of this virus in case it infects a system, the following steps should be followed: (a) isolate the infected system (i.e. cut the computer off from the network); (b) check the computer's data (i.e. the user should check for data corruption on the hard drive); (c) analyse the code and its operation; (d) remove the virus manually; (e) contact the creators (i.e. thanks to the personal data included in the message of the virus); (f) alert the community.

The Morris virus appeared in 1988,[16] created by Robert Tappan Morris, who studied at Cornell University. This virus was assessed as having significant capabilities to attack targets on the Internet, and its purpose was to spread across computer networks to study the rules governing the spread and structure of the Internet. Thus, this program was still not aimed at data theft or information destruction. The attacks of the Morris virus spread worldwide across numerous computer stations owing to poorly secured passwords, email program vulnerabilities, and finger program errors. The consequences of these attacks were the paralysis of many systems and the infection of computers, which experienced difficulties in booting. Owing to such activities, society has become more aware of the importance of IT security strategies, and many system protection tools and strategies have been developed.

Regarding the management of this virus in case it infects a system, the following steps should be followed: (a) isolate the system (i.e. disconnect the computer from the network); (b) change passwords (i.e. especially accounts with weak passwords); (c) update and secure the software (i.e. to prevent vulnerabilities in programs, including Internet emails); (d) perform virus analysis and removal (i.e. including manual removal of infected files and system cleaning); (e) report the incident (i.e. to appropriate institutions or Internet service providers).

15 Thomson and Nichols, 2009.

16 *The Morris Worm: 30 Years Since First Major Attack on the Internet*, 2018.

The attack on Microsoft[17] took place in 1995 by Kevin Mitnick, a hacker who broke into Microsoft's computer systems, configuring the first serious hacker attack in the context of computer security. The hacker was subsequently found and arrested in the same year. In fact, during the 1980s and 1990s, Mitnick also hacked into the computers of various other companies. After his arrest, the talented criminal decided to change the direction of his actions and started engaging in legal work and computer security, eventually becoming an expert in the field.

The DDoS attacks during the Y2K Crisis took place in 2000,[18] with the literature on the subject focusing mainly on problems related to the transition of computers from a two-digit year to a four-digit year during the Y2K Crisis. This was a problem related to time counting, and during this specific period, we still did not have advanced tools to monitor and take action to detect these incidents, nor awareness in this area.

The cyberattacks on Estonia occurred in 2007,[19] and were the first of their kind. It was the result of political disagreements between Russia and Estonia on from the relocation of a Soviet monument located in Tallinn, Estonia. The DoS attacks were then organised and carried out by the Russian organisation "Nasi" and independent Russian hackers. An important context is that Estonia had switched to making payments only via an electronic system and withdrawn traditional money from circulation in the country right before the cyberattacks, meaning that the cyberattacks could easily destabilise the functioning of the state. The perpetrators attacked sectors of the state government such as the following: (a) financial sector, causing people to be unable to perform financial operations and access bank accounts; (b) governmental sector, causing the blocking of the websites of the parliament, Ministries of defence and justice, political parties, uniformed services, and education; (c) defence sector, blocking access to the websites of the Ministry of Defence and forcing the Estonian defence system to close some foreign connections; (d) tourist sector, as Estonian people traveling abroad could not access their bank accounts, and foreign offices had their booking systems for trips to Estonia blocked; (e) media sector, as it was not possible to post information on websites nor to modify websites; (f) the infrastructure sector.

The consequences of these attacks were cutting off Estonia from the rest of the world, blocking the flow of financial resources, manipulating the contents posted on government websites, and paralysing services. Estonians could not lead their daily lives normally, leading to chaos and tension in the national society. Therefore, this attack showed, for the first time, and as Estonian President Toomas Hendrik pointed out live in his statement, that 'Nowadays, infrastructure can be destroyed online, it does not require missiles'. Despite the whole dire situation, Estonia did not report

17 *Microsoft Faces Blistering Attack On-Line Leaders Say Software Giant Wants To Extend Its Dominance*, 1995.

18 *Y2K bug*, no date.

19 *A look at Estonia's cyber attack in 2007*, 2009.

on major financial losses owing to the events. The response to this series of issues was the development, in Estonia, of robust defence capabilities to respond to this type of threat and attack. In fact, the literature on this subject indicates that Estonia has become a pioneer in cybersecurity, and has significantly increased its financial outlays on resources and well-qualified experts on cybersecurity. Internationally, the incident drew the world's attention to this new, very real threat, leading to an increased awareness of the need to immediately strengthen defence systems, both at the technical and political levels, in the cyberspace.

Regarding the management procedures necessary in case of such cyberattacks, the following steps should be followed: (a) activate the cyberspace defence system (i.e. identify the origin, type, and purpose of the attackers) and improve security (i.e. after analysis, weak points should be checked actions taken to seal them); (b) government entities should provide an immediate response (i.e. resource security should be established, and the targets of the attacks and potential consequences should be determined); (c) establish crisis communication (i.e. a safe communication channel should be established for securing cooperation and communication between the government, society, the media, and spokespeople for security entities); (d) promote international cooperation (i.e. international partners and allies should be informed about the attack and cooperation with the Security Agencies of other countries should be confirmed); (e) increase defence capabilities (i.e. the institution's/state's defence strategy should be developed, and financial expenditure on the development of cybersecurity and common action strategies should be increased).

The Stuxnet attack occurred in 2010,[20] with the Stuxnet malware having been created as part of Operation Olympic Games, which aimed to attack Iran's nuclear program. It was part of the operation that attacked the Supervisory Control and Data Acquisition (SCADA) systems, entered false data into these systems, and took control of the industrial equipment of Iran. One of the first iterations of this malware was used to spy on and reprogram the industrial installations associated with Iran's nuclear program. It used zero-day exploits, that is, unknown errors in the software. According to both the literature on the subject and the experts interviewed, this was the first cyberattack on a critical global infrastructure, and led 2,000 of the 8,700 centrifuges used by Iran to be replaced. No country or organisation has ever admitted to having been part of this operation, but suspicion has been directed towards the intelligence agencies in the United States of America and Israel. Iran's lost credibility in the world stage in the context of its nuclear program, owing to this attack. Therefore, the Stuxnet allowed for an advanced attack that disrupted the operation of industrial control systems, led countries and organisations worldwide to intensify their work on IT security, and sparked international discussions on ethics and the consequences of cyberattacks on critical infrastructure.

Regarding the management procedures necessary in case of such cyberattacks, the following steps should be followed: (a) analyse the malware; (b) restore the system

20 Falliere, O Murchu and Chien, 2010.

using a backup; (c) update the system; (d) monitor network flows; (e) strengthen security; (f) cooperate with cybersecurity experts; (g) promote employee education.

The ransomware attack on Target occurred in 2013[21] in the United States of America. Despite the name commonly afforded to the event, this was an incident and not a ransomware attack. Specifically, hackers managed to illegally access the computer systems of Target, a large retail company in the United States of America, leading to the compromise of the financial and personal data of over 40 million customers. The incident was focused extracting information about the company's payment systems and using the customer data for making other unauthorised payment transactions.

Regarding the management procedures necessary in case of such attacks, the following steps should be followed: (a) isolate the system; (b) report the incident; (c) assess the scope of the incident; (d) identify the incident; (e) stop the attack; (f) restore the system using a backup; (g) analyse payments made during the event; (h) analyse the causes of the incident; (i) implement preventive measures; (j) inform the affected parties; (k) promote employee education.

The WannaCry attack occurred in 2017,[22] and was estimated to be the largest attack of this type in history, affecting nearly 300,000 computers in over 150 countries. This malicious ransomware encrypts files on infected computers and then demands a ransom in the form of Bitcoin cryptocurrency for victims to receive the password to decrypt the files. This attack was characterised by the use of an exploit, called "EternalBlue", focused on vulnerabilities in the Windows operating system, which not only spread quickly but also infected various computers on the same network. This attack was performed at the global scale, affected many countries, and was targeted at government entities that focused on guaranteeing national security. It is described that this exploit had been previously created by the intelligence agency at the United States of America. The consequences of the attack included the closure of very important institutions for various countries worldwide, such as those described herein: the British health service, national railways and banks in Russia and over 1,000 computers in the Ministry of Interior of Russia, Indian airlines, universities in Italy, and various companies (e.g. MegaFon, EMERCOM, Nissan Telefonica, Deutsche Bahn), hospitals, and units in public institutions. Thus, the attack destabilised and disrupted state functioning, and resulted in enormous economic and social costs, as both entrepreneurs and state institutions were forced to pay a ransom in exchange for their own data.

The attack gave further fuel for the expansion of discussions surrounding cybersecurity, and led to the onset of digital security analyses involving not only threats but also management and liability issues. The theft by hackers of a tool originally created by an intelligence agency made us realise that this type of tool may eventually fall into the hands of organised criminal groups, rendering it important for

21 Gopal, 2022.
22 *What is WannaCry ransomware?*, no date.

security stakeholders to also have access to able to destroy such products. This attack also urged institutions to emphasise the development and introduction of procedures to counteract such negative phenomena, such as by promoting the regular updating of operating systems, the implementation of effective solutions (e.g. firewalls, antivirus programs), and greater financial and material expenditure on cybersecurity.

Regarding the management procedures necessary in case of such cyberattacks, the following steps should be followed: (a) isolate the system; (b) stop network traffic; (c) inform security entities; (d) inform the staff; (e) launch a procedure in the event of a ransomware attack; (f) report the incident to security units; (g) determine the source of the attack; (h) identify suspicious activity on the network; (i) check for system updates; (j) activate additional security measures, such as firewall and antivirus programs; (k) inform and warn the public; (l) backup security; (m) restore systems to pre-attack levels; (n) monitor cryptocurrency payments; (o) analyse the attack; (p) prepare and present a report; (r) promote staff education; (s) educate the public; (t) implement the developed solutions; (u) cooperate with security entities.

The SolarWinds attack took place in 2020,[23] and was deemed one of the most advanced cyberattacks to date. It targeted the SolarWinds company, which focuses on software for monitoring networks and IT systems, aiming to break into their IT systems. Access to the systems of the clients of the company was possible by introducing a malicious software update code. The attack was aimed at obtaining confidential data from government institutions, technology companies, and other industrial sectors, indicating that the operation had espionage purposes. This incident gave way to the awareness of the leaky conditions of supply chain systems and their vulnerabilities to attacks, causing companies using this type of supply chain management system to run detailed analyses of their internal security strategies. So far, the focus of these attacks has been on internal issues and not on the product delivery process.

Regarding the management procedures necessary in case of such cyberattacks, the following steps should be followed: (a) disconnect the systems; (b) notify security entities; (c) alert staff; (d) secure resources; (e) analyse losses; (f) analyse the attack source; (g) change passwords and keys; (h) check backups; (i) implement system updates; (j) monitor the situation; (k) counteract further attacks; (l) update software and use anti-virus programs and firewalls; (m) promote staff education; (n) promote public education; (o) cooperate with security entities; (p) prepare a report after analysing the situation; (r) verify procedures; (s) update procedures; (t) implement procedures; (u) conduct risk analysis.

23 Oladimeji and Kerner, 2023.

3. Cyberattack types

Based on many years of experience related to computer development and cyberattacks, stakeholders have created several categories of cyberattacks, which continue to evolve and expand to this very day and as reality changes. According to Grzelak and Liedl, the most common threats in the cyberspace are the following:[24] (a) attacks using malicious software (e.g. malware, viruses, and worms); (b) identity theft; (c) theft (extortion) and data modification or destruction; (d) blockage of service access (e.g. mail bombs, DoS, and DDoS[19]); (e) spam (i.e. unwanted or unnecessary electronic messages); (f) social engineering attacks (e.g. obtaining confidential information by impersonating a trustworthy person or institution, also known as phishing).

Threat identification is at the foundation of prevention efforts against cyberattacks, enabling institutions to prepare for these eventualities through the effective implementation of protective measures and safety procedures. Therefore, a Catalogue of Information Security Threats is provided in this section, listing threats to information security (e.g. cyberattacks, threats caused by human activity, security vulnerabilities, software errors) and describing the risks that they pose regarding loss of data confidentiality, integrity, and availability.

The catalogue comprise cyberattacks related to the following, although it is important to emphasise that new types of cyberattacks are constantly being evaluated and are likely to enter future catalogues: (a) malware, (b) phishing, (c) ransomware, (d) DDoS attacks, (e) attacks on industrial control systems (ICS) and SCADA systems, (f) attacks on web applications, (g) attacks on wireless networks, (h) attacks on Internet of Things (IoT) systems, (i) email attacks, (j) password and authentication attacks, (l) attacks on critical infrastructure, (m) attacks on mobile applications, (n) attacks on blockchain and cryptocurrencies, (o) system hacking, (p) data disclosure, (r) internal threats, and (s) network security incidents.

Malware (e.g. viruses, Trojans, spywares, and computer worms): (a) the virus is a malicious code that attacks healthy files, infects programs, and can be compared to a biological virus that needs a host for replication; (b) computer worms are very similar to computer viruses (except that they do not need a "host for replication" and instead can self-replicate), generally operate on the Internet, and can be transferred via portable memory; (c) Trojans, also known as Trojan horses, work under the guise of a useful application and have a wide scope applications, being useful for deleting specific system files, intercepting information entered via the keyboard, or using the computer to send spam.[25]

Phishing involves attempts at obtaining confidential personal information by using the guise of a trusted person or a credible institution. A characteristic of this activity is the need for the quick provision of information, which leads phishing procedures to induce specific, quick actions by the victim for the computer to be

24 Grzelak and Liedel, 2012, p. 131.
25 Nowak-Brzezińska, 2017, p. 19.

infected with a Trojan or spyware. Phishing can take the form of a message sent via email or an instant messenger, persuading the user to click on a link containing a fake organisational website. This applies mainly to banks. This type of cyberattack aims at collecting personal data and persuading people to download Trojan software. Perpetrators make every effort to ensure that the situation generated is as credible as possible.[26]

The ransomware is a type of malware aimed at infecting and/or blocking a computer system by stealing and encrypting selected files. It is a type of fraud aimed at extorting funds from victims in exchange for the lost data. Ransomwares hence not only encrypt the data but also steal it, and tend to be used especially on attempts at acquiring classified, sensitive datasets that would lead to embarrassment, especially for public sector representatives, in case disclosed. After a ransomware attack is successful, data recovery is only possible using a decryption key, for which the perpetrators demand a ransom.[27]

DoS and DDoS attacks[28] involve blocking access to the service by taking up all free resources (e.g. flooding a service with excessive amounts of data or queries), leading to system overload and suspension.

Attacks on ICS and SCADA systems focus on critical infrastructure violation and are made viable through the exploitation of security vulnerabilities that enable system manipulation. This practice disrupts production, destroys equipment, and causes failures, leading to serious consequences such as power outages and physical damage to infrastructure. Protection against this type of attacks is possible by using advanced security solutions, including network monitoring, system segmentation, and regular security updates.[29]

Attacks on web applications are attempts at gaining unauthorised access to, modifying, or destroying applications available online. Methods such as SQL injection, cross-site scripting (also known as XSS), and cross-site request forgery (also known as CSRF) are used to break app security and gain access to data. Related activities are often aimed at stealing information, changing the application's functions, or infecting it with malware. Effective protection against these attacks requires constant application security monitoring, penetration testing, and security measure implementation (e.g. application firewalls and two-factor authentication mechanisms).[30]

Attacks on wireless networks target radio communication infrastructure, and the most frequently used methods are man-in-the-middle attacks, de-authentication, and breaking encryption keys. The goal of such attacks is often to take control of the network, access data, or eavesdrop on communications, and they take advantage of gaps in security protocols such as WPA2. The use of strong encryption methods,

26 Nowak-Brzezińska, 2017, pp. 21–22.
27 *Poradnik ransomware* [Guide ransomware], no date.
28 Based on European Court of Auditors, 2019; *Cybersecurity: how the EU tackles cyber threats*, no date.
29 Liderman, 2020, p. 6.
30 *Ataki na aplikacje webowe. Jakie są najczęstsze i jak się bronić?* [Attacks on web applications. What are the most common ones and how to defend yourself?], 2022.

constant network traffic monitoring, and constant device and system updates can protect against such attacks to some extent.[31]

Attacks on IoT systems focus on devices and networks integrated with IoT, and attackers exploit vulnerabilities in devices such as cameras, sensors, and home devices in attempts to gain unauthorised access or control over, or even to steal, data. These types of attacks often relate to espionage, disrupting device functions and violating users' privacy. Methods of protection against such attacks include strong authentication mechanisms, data encryption, software updates, and network activity monitoring.[32]

Email attacks are used by cybercriminals and customarily involve the use false links inside email contents or attachments with the purposes of data theft, system infection, privacy breach, among others. Protection against this type of attack is possible through increasing user awareness, knowledge about cyberattack mechanisms, and making use of antivirus programs.[33]

Password and authentication attacks involve breaking access security mechanisms. The methods used are often brute force, dictionaries, and data leaks to test the same authentication data in other services. Phishing and keyloggers form additional threats used for conducting fraud and sending malware for the purpose of intercepting confidential information. Defence against this type of attack is possible by using strong passwords, two-step verification procedures, monitoring login activity, changing passwords, knowledge of how this type of cyberattack works, and having the ability to react in the event of an attack.[34]

Attacks on critical infrastructure focus on compromising the systems and resources necessary for the functioning of society and state security, including key industrial sectors such as energy, transport, communication. Methods include cyberattacks on industrial control systems, sabotage, and terrorist acts, and examples of consequences include energy supply disruptions, transport disruptions, and communication system failures. The security of critical infrastructure requires complex defence strategies, robust cybersecurity measures, and international cooperation.[35]

Attacks on mobile applications encompass methods such as reverse engineering, code injection, and man-in-the-middle attacks, and tend to lead to personal data theft, unauthorised access to private information, and malware infections. These attacks are possible due to security vulnerabilities in the applications or operating systems. Actions to counteract these attacks include programming practices, data

31 Waraksa, Żurek and Niski, 2011, p. 88.

32 *Internet Rzeczy, ochrona prywatności a bezpieczeństwo danych* [Internet of Things, privacy protection and data security], 2021.

33 *Phishing: co to jest?* [What is phishing?], no date.

34 *Czym jest uwierzytelnianie dwuskładnikowe, uwierzytelnianie dwuetapowe?* [What is two-factor authentication, two-step authentication?], 2023.

35 Barć, 2021, p. 7.

encryption, updates, and activity monitoring to minimise the risk of attacks on mobile applications.[36]

Attacks on blockchain and cryptocurrencies attempt to violate the integrity and security of these technologies, with attackers using various methods (e.g. double spending, 51% attack, and Sybil attack) to introduce disinformation, disorganisation, take control of the network, manipulate transactions, promote financial fraud, and fund theft. Additional threats include smart contract vulnerabilities, phishing among cryptocurrency users, and attacks on stock exchanges. Security against such attacks is achieved through the use of solid security protocols, code audits, user education, and blockchain network activity monitoring.[37]

System hacking refers to the illegal process of accessing computer systems to manipulate or breach them, steal confidential information, change system settings, introduce malware, crack passwords, solve authentication mechanisms, and using exploits. It often involves methods like security vulnerability exploitation, buffer overflow attacks, and gaining illegal access to data. The effects of system hacking can be serious, with consequences ranging from loss of privacy to organisational operation disruption. Effective protection involves developing appropriate security measures, system updates, and network activity monitoring.[38]

Data disclosure encompasses the accidental or illegal disclosure of confidential or private information (e.g. personal and customer data or confidential documents) to the public, with major reasons being security system errors, data leaks, or intentional attacks. The consequences of data disclosure include identity theft, privacy breaches, and financial losses. Counteracting this type of incident is possible by using strong security measures, monitoring data, and complying with appropriate regulations regarding personal data protection.[39]

Internal threats are generated intentionally (e.g. data theft, sabotage, and corporate crime) or unintentionally (e.g. error or lack of employee knowledge) by company employees with access to specific resources or security measures. These actions can result in leaks and loss of data or other damages. Countermeasures include regular employee training, raising awareness of risks, and using modern technological security measures.[40]

A network security incident is an unwanted or illegal incident that affects data integrity, availability, or confidentiality on a computer network, the consequences of which may include attacks, data leaks, loss of access to the system, system failures, financial losses, loss of company reputation, and privacy invasion. Effective

36 Niewiadomska-Szynkiewicz and Litka, 2023, pp. 96–99.

37 *Blockchain – aspekty techhnologiczne oraz przykłady zastowań* [Blockchain – technological aspects and examples of applications], no date.

38 Pala, 2015, pp. 115–116.

39 *Naruszenie ochrony danych przez podmiot przetwarzający. Czym jest i jak postępować, kiedy do niego dojdzie* [Data protection breach by the processor. What is it and what to do when it happens], 2021.

40 European Union Agency for Cybersecurity, 2020a.

countermeasures include applying a network security policy, monitoring network traffic, and increasing employee awareness.[41]

A catalogue of information security threats should be created, made open for all stakeholders, and be constantly updated, with especial attention to areas that can destabilise state functioning in case of disruption, namely: (a) data and privacy attacks, (b) attacks on government institutions and enterprises, (c) on delivery companies, (d) on social media, and (e) on data processing systems.

Data and privacy attacks are aimed primarily at access, theft, and manipulation of business and/or private databases, with customary methods being phishing, malware, and security vulnerability exploitation. The consequences of these attacks are financial losses and the violation of rights at the personal and/or business level.[42]

Attacks on government institutions and enterprises often attempt to violate their structures or penetrate them, and tend to involve organised criminal activities focused on destabilising entities that constitute the state security system and/or the economic sector. The methods used for this type of activity include cyber intrusions, phishing, and ransomware. Acquiring governmental data often associates with ransom requests, obtention of confidential information to be passed on for hostile entities or countries, and system operation disruption. Attacks of this type are particularly dangerous and therefore require complex security strategies, constant monitoring, employee education, and intersectoral cooperation for a coordinated response to possible threats.[43]

Attacks on delivery companies aim at disrupting transportation and delivery operations. Attackers who want to disrupt the supply chain may use various strategies, such as cyber intrusions, ransomware, or fake advertisements. Targets may include logistical data, shipment data, and ransom demands for the release of blocked shipments. The consequences of this type of attacks are supply interruptions, the consequential financial losses, and data losses. Protection against this type of attack requires the use of IT security measures, the monitoring of logistics traffic, and educating employees on cybersecurity.

Attacks on social media are often performed through hacking, phishing, and DDoS attacks, and tend to aim at disrupting activities or taking control of social media platforms. Successful attacks may then lead to the publishing of false information, and the creation of false scenarios that then discredit people and/or organisations. The main goals tend to be information manipulation, disinformation,

41 Pacut, 2023.

42 Zhu et al., 2018.

43 Based on (2024) List fifteen the largest threats. [Online]. Available at: https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-enisa-list-of-top-15-threats-ebook-en-pl.pdf and (2024) ENISA Threat Landscape 2021. [Online]. Available at: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_pl.pdf (Accessed: 10 January 2024) and (2024) Vademecum of information security. [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/ (Accessed: 06 January 2024), p. 22.

industrial espionage, and achieving financial gains through data theft or blackmailing. These attacks affect user security, information credibility (e.g. especially of public figures), and the trust and credibility of companies. Protection against them requires effective cybersecurity measures and the monitoring of online activity and user education.

Attacks on data processing systems are aimed at disrupting the operation of infrastructure that processes information or obtaining the related data. The techniques used security vulnerability exploitation, SQL injection, and malware attacks. Common consequences involve data confidentiality losses, operational system disruptions, and financial losses. Prevention measures include the implementation of effective safeguards, monitoring activity, regular updates, and educating employees about cybersecurity.

4. Major cyberattacks threatening security

Cyberattacks are very dangerous because they do not recognise any territorial boundaries. Examples include the decisions over the attacks being potentially made in places like Moscow, Beijing, or Pyongyang, whereas the operations or cyber activities themselves may use IT networks located anywhere in the world. Cyberattacks can be broadly divided into four categories, as follows:[44] (a) interception, involving attacks against confidentiality; (b) interruption, involving attacks against availability or usability; (c) modification, involving attacks against availability and usability; (d) fabrication, involving attacks against authenticity. Importantly, cyberattack risks exist when there are threats, which in turn are created through cybersecurity vulnerabilities and gaps.

Cybersecurity is a field under development and is characterised by being dynamic. Furthermore, in order to control the emerging phenomenon of cyberattack, many institutions have developed various reports on cyberattacks. To secure data reliability, this study used data presented by the European Union Agency for Cybersecurity (ENISA) from 2022.[45]

44 Based on European Union Agency for Cybersecurity, 2020b; European Union Agency for Cybersecurity, 2021; Cendrowski, 2020, p. 22.

45 *European Union Agency for Cybersecurity (ENISA)*, no date.

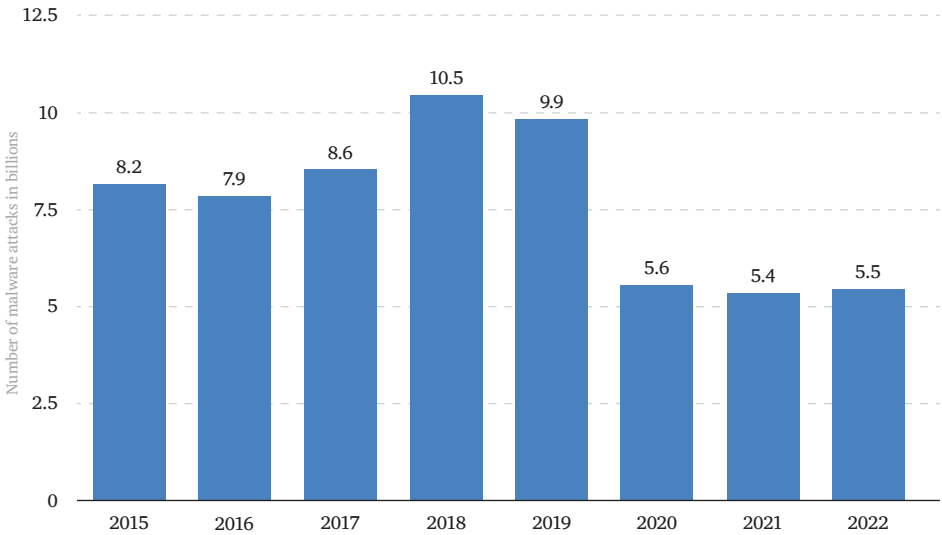
Figure 1.[46]

There are many threats on the Internet, with both experts and the ENISA reporting[47] the following as major ones. First, ransomwares, which are the most disturbing because hackers are increasingly using more sophisticated and aggressive techniques to acquire ransom for restoring access to accounts and data. The average ransom value has more than doubled in just one year (2019, EUR 71,000; 2020, EUR 150,000), and 2021 saw a 57-fold increase in ransom requests compared to 2015, reaching a value of EUR 18 billion. Second, malwares, which target systems and include spywares, Trojan horses, viruses, and worms. Statistics and commentaries are presented below the chart.

46 *ENISA Threat Landscape 2022*. [Online]. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, p. 10 (Accessed: 10 February 2024).
47 European Union Agency for Cybersecurity, 2021.

Figure 2.[48]

Annual number of malware attacks worldwide from 2015 to 2022 (in billions)



Source
SonicWall
© Statista 2023

In 2022, the number of malware attacks worldwide reached 5.5 billion (an increase of 2% compared to the previous year), while 2018 saw the highest number of malware attacks in recent years, when 10.5 billion such attacks were reported worldwide.[49] In the same year, malwares were blocked more than 205 million times, and a popular type of malware targeted mainly the Asia-Pacific region. In general, websites are the most common vector for malware attacks, and recent industry data has shown that malware attacks were often received via exe files.[50] A decline in this threat was observed only during the COVID-19 pandemic.

Moreover, the emergence of the so-called cryptojacking activities, which aim at using the victim's computer equipment without his/her knowledge to steal cryptocurrency, resulted in a significant increase in the number of cyberattacks. For example, considering only the first half of 2022, there was a four-time increase in attack numbers compared with the numbers in the previous four years.[51]

48 *Annual Number of Malware Attacks Worldwide from 2015 to 2022.* [Online]. Available at: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/ (Accessed: 10 January 2024).
49 Petrosyan, 2024.
50 Ibid.; European Court of Auditors, 2019.
51 Petrosyan, 2024.

There are also threats related to social engineering, which includes persuading people to open documents and visit websites that unknowingly make their own systems and services available for access to others. These initiatives involve both intentional and unintentional human behaviours, and the most frequently used techniques are phishing (through emails) and smishing (through SMS). In Africa, Europe, and the Middle East, approximately 60%[52] of network security breaches made possible through social engineering were reported. The hackers mainly impersonated financial and technology sector specialists to attack cryptocurrency exchanges and their owners.

Other threats include data breaches, with 82% of the recorded data security breaches being associated with human activity, mainly with human errors. These threats can be divided into (a) data security breaches (intentional actions) and (b) leaks (unintentional actions). The main reasons for data breaches were the desire to obtain funds at 90% and espionage at (10%).

Accessibility threats should also be mentioned, including (a) DDoS attacks, which are very complex, encompass a wide range of activities, are targeted at mobile networks, have been often used in the Russian–Ukrainian war, and also take place on the network. These types of attacks were also used against websites containing information about COVID-19 vaccinations. Another threat relates to (b) efforts at destroying Internet accessibility, with one example being the Russian–Ukrainian war, where 15% of the Internet infrastructure in Ukraine has been destroyed[53] since its onset. Censorship has also been imposed on social media and news portals.

Disinformation, referring to the use of the mass media to transmit false information in order to cause fear, uncertainty, and chaos in society and among nations, is another a significant threat. This method has been used by Russia in relation to information regarding the course of their invasion in Ukraine. The use of wide-scale disinformation methods is also becoming more common with the advent of artificial intelligence, deepfake technology (i.e. creating false recordings, images, and sounds indistinguishable from the original ones), bots (i.e. capable of pretending to be people), and threats to the supply chain (i.e. to obtain customer data and to attack the supplier and the recipient; these attacks are becoming increasingly easier owing to the different number of suppliers).

4.1. Sectors of life at risk

Cyberattacks affect public sectors and people's lives at varying intensities. Based on research conducted by the ENISA regarding reported cyberattacks from July 2021 to June 2022, there are seven areas where these attacks occurred most frequently, which are the following:[54] (a) public administration/government (24%), (b) digital

52 *Cyberbezpieczeństwo: główne i nowe zagrożenia* [Cybersecurity: main and new threats], 2022.
53 *Cyberbezpieczeństwo: główne i nowe zagrożenia* [Cybersecurity: main and new threats], 2022.
54 Petrosyan, 2024.

service providers (13%), (c) society (12%), (d) services (12%), (e) finance/banking sector (9%), (f) healthcare (7%), (g) and other areas (23%).

4.2. Most frequently attacked industries

In 2022, the education sector was heavily attacked by malwares, with an average of 2,314 attacks per week and more than five million malware attacks. This sector was followed by government and military organisations and then healthcare units.[55]

4.3. Costs

These cyberattacks are estimated to have led to huge financial losses, albeit the losses and damages are not restricted to finance and instead extend to the personal and social levels. Based on the data presented in the European Union (EU) Report, the following costs were incurred.[56] First, it was for the economy, as small and medium-sized enterprises in the EU do not feel safe in the EU digital market, and this is despite its design to ensure confidence and security on the Internet. This lack of sense of safety results from the fact that, by the end of 2021, 28% of the recorded cyberattacks in the EU had targeted small and medium-sized enterprises, and this number is constantly growing. Second, for democracy, as disinformation causes trust losses in society and leads to divisions. Third, for peace and security, as data manipulation (e.g. through the use of bots and disinformation activities) affects the democratic resilience of countries and introduces chaos and tensions. According to ENISA data, during the Russian–Ukrainian war, cyberattacks were carried out in parallel with conventional fighting methods in an attempt to disrupt the capabilities of government agencies and entities and lead to trust losses among the public, especially in political leadership. Fourth, for essential services and critical sectors such as health, finance, transport, energy, water, and gas, which are dependent on digital technology and devices connected to different networks. Owing to such dependence, interference in their functioning offers risks to life and health. Hospitals also saw disruptions in their care systems, cancelled/interrupted surgeries, and there were threats to the supply of services. There were also threats associated with the use of smart homes and devices.

55 Petrosyan, 2024.
56 *SMEs and Cybercrime*, 2022.

5. Causes and effects of cyberattacks: A summary

As shown above, the catalogue of cyberattacks contains numerous entries. The table below presents the following types of cyberattacks: malware; phishing; ransomware; DDoS attacks; attacks on industrial control systems; attacks on web applications; attacks on wireless networks; attacks on IoT systems; email attacks; password and authentication attacks; attacks on critical infrastructure; attacks on mobile applications; attacks on blockchain and cryptocurrencies; system hackings; data disclosure; internal threats; network security incidents; data and privacy attacks; attacks on government institutions and enterprises; attacks on delivery companies; attacks on social media; attacks on data processing systems.

Importantly, each cyberattack has specific capabilities and is used for a specific purpose, the reasons for using various types of cyberattacks may sometimes be the same, and the choice of a specific cyberattack depends on the knowledge, skills, and technical capabilities of the perpetrators of cyberattacks. Each form of cyberattack has specific negative consequences that may affect the functioning of the public, families, social groups, the government and, consequently, the state. They can be used to disrupt or destroy many areas important for the state or citizens. The table below shows cyberattack types, the reasons for their use, and the consequences in all possible areas. Presenting the data in this form allows for comparisons regarding the degree of danger of individual forms of cyberattack.

In summary, the main reasons for using cyberattacks are the desires of perpetrators to achieve financial benefits, destabilise the functioning of the government, enterprises, and competition, and obtain sensitive information from various sectors (e.g. financial, economic, governmental sectors). As a consequence of cyberattacks, chaos, disinformation, and tensions arise among society. All this contributes to the destruction of states from within, making them easy targets for aggressors to attack.

Table 1.

Cyberattack type	Reasons	Consequences
Malware	– trying to earn money – trying to harm a person/ company/country – controlling computers/mobile devices for illegal purposes – taking control of devices to attack other entities	– destruction, acquisition, or deletion of data – spying or controlling computer systems – taking control of devices – computer attacks on other organisations through a victim organisation

Cyberattack type	Reasons	Consequences
Phishing Phishing attack	– extorting confidential personal information – financial fraud	– loss of identity – loss of sensitive data – insults and embarrassments – loss of financial resources – obtaining confidential data – taking over databases – loss of image – cyberstalking – loss of trust (e.g. customers) – destabilisation – loss of market positions
Ransomware	– extorting payment for removing the infection – extorting confidential information	– loss of financial resources – loss of control over devices – taking over databases – obtaining confidential data
DDoS attack	– occupation of system resources (e.g. server, memory, and power) – preventing the functioning of a given service on the Internet – preventing the use of a given Internet domain – attempting to eliminate competition on the market	– loss of customers – loss of image – loss of trust (e.g. customers) – interruptions in the operation of trading systems (financial losses)
Attacks on industrial control systems	– trying to earn money – preventing the operation of a given enterprise – attempting to steal digital data	– breach of trust in the enterprise/organisation – leakage of unfavourable data to the public – sales of digital data – disturbance in the functioning of production processes – disturbance of functioning of the population regarding needs related to activities of daily living
Attacks on web applications	– stealing data (e.g. customers and application users) valuable to hackers	– financial losses – weakening the brand image – loss of user trust – data leakage of sensitive application users – loss of confidential data

Cyberattack type	Reasons	Consequences
Attack on wireless networks	– stealing confidential data for illegal purposes – stealing bank account details – stealing passwords and taking over user accounts on websites	– loss of privacy and data security – loss of financial resources and control over finance on banking websites – leakage of sensitive user data – loss of passwords, accounts, and control over the device and websites
Attacks on IoT systems	– taking control of IoT devices and causing damage to them, or using them in attacks on more targets – spying and blackmailing device users – extorting through access to confidential information	– loss of control over the IoT device – data breach or loss by device users – sensitive data leakages – insulting and embarrassing – cyberstalking – loss of privacy and security
Email attacks	– stealing email accounts to extort funds and/or confidential information – stealing email data	– breach or loss of confidential or sensitive data – financial losses – cyberstalking – disruption of internet operations – loss of passwords, accounts, and control over the device
Password and authentication attacks	– extorting confidential personal information – phishing sensitive data	– loss of passwords, accounts and control over the device and websites – loss of sensitive data – loss of confidential data – insulting and embarrassing – loss of good name

Cyberattack type	Reasons	Consequences
Attacks on critical infrastructure	– disrupting the country's/institution's activities – causing market confusion – stimulating social unrest – loss of trust in government/institutions – spreading disinformation to destabilise the state – weakening of the economy	– disruption of the operation of critical infrastructure systems (e.g. emergency services, healthcare, energy supply, communication and information and communication technology networks, financial, water and food supply, transport, production, and administration) – destabilisation of critical infrastructure key to state security and citizens – destabilising the functioning of state economy – weakening social security – social unrest – insulting, discrediting, and loss of trust
Attacks on mobile applications	– stealing data (e.g. customers and application users) valuable to hackers – stealing bank details – stealing passwords and taking over application accounts	– financial losses – loss of accounts in applications – loss of control over data in the application by the user – cyberstalking – weakening the brand image – loss of user trust – data leakage of sensitive application users – loss of confidential data
Attack on blockchain and cryptocurrencies	– stealing funds – disrupting the financial market – strengthening one cryptocurrency at the expense of the other	– loss of financial resources – leakage of sensitive data – loss of access to financial resources – elimination of competition

Cyberattack type	Reasons	Consequences
System hackings	– gaining access to the system and its resources – obtaining confidential and sensitive data – disrupting the system	– loss of access to the system and its resources – loss of confidential data – loss of sensitive data – breach of confidential data and system availability – insulting and embarrassing – loss of financial resources – taking over databases – destabilisation – loss of market position
Data disclosure	– stealing confidential and sensitive data and databases – stealing funds – stealing bank details	– loss of confidential data – loss of sensitive data – loss of databases – loss of financial resources – insulting and embarrassing – loss of customers – loss of image
Internal threats	– stealing bank details – stealing confidential data – stealing databases	– loss of confidential data – loss of sensitive data – loss of databases – loss of financial resources – destabilisation
Network security incident	– obtaining confidential data – disrupting system integrity	– loss of data confidentiality – loss of financial resources – irregularities in the operation of security systems
Data and privacy attacks	– identity theft – obtaining confidential and sensitive data	– loss of sensitive data – loss of identity – loss of image – taking over databases – insulting and embarrassing – loss of financial resources – cyberstalking

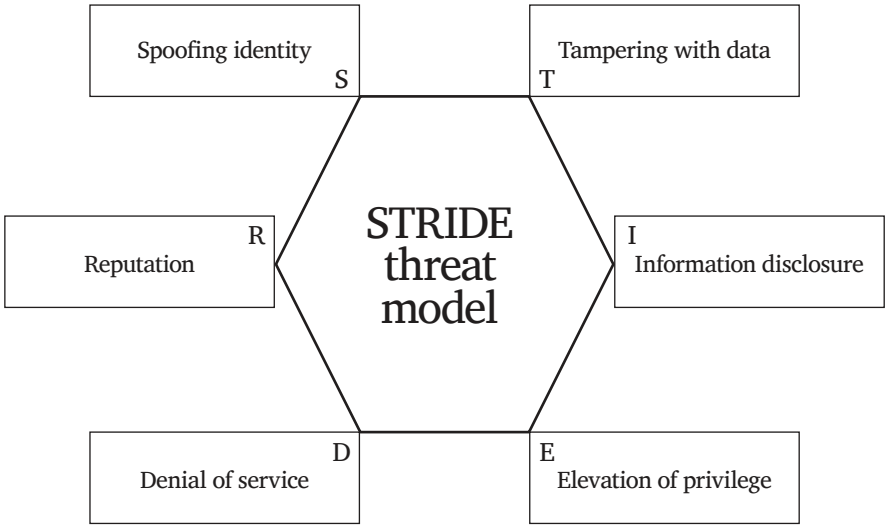
Cyberattack type	Reasons	Consequences
Attacks on government institutions and enterprises	– disrupting the country's/institution's activities – disrupting the activities of financial institutions – causing market confusion – causing social unrest – loss of trust in the government/institution – spreading disinformation to cause destabilisation – weakening of the position and trust in the institution/government – weakening of the economy	– loss of databases – loss of confidential data – destabilisation of the institution/country – duplicating fake news campaigns (e.g. for disinformation and/or social unrest purposes) – insulting and compromising – loss of trust (e.g. customers and/or citizens) – customer acquisition – financial losses – loss of market position – loss of image
Attacks on delivery companies	– weakening of the economy – extorting confidential personal data – fraud of payment card details – taking over bank data – obtaining financial resources	– loss of bank details – financial losses – loss of personal data – loss of confidential data
Attacks on social media, websites	– stealing sensitive data – stealing bank details – stealing passwords and taking over application accounts	– loss of passwords and accounts – financial losses – loss of sensitive data – loss of confidential data – insulting and embarrassing – loss of image – cyberstalking – loss of control over data in the application by the user
Attacks on data processing systems	– takeover of databases – interception of confidential and sensitive data – taking over bank details	– loss of sensitive and confidential data – insulting and embarrassing – loss of financial resources – taking over databases – loss of image – destabilisation – loss of market position

6. Cyberspace as a combat place

As mentioned above, cyberspace has been recognised as the fifth battlefield dimension where war can take place. This dimension is special because its users are anonymous and may often feel unpunished. Importantly, special technologies have been created to increase anonymity on the Internet (e.g. the Onion Router, also known as TOR) or proxies, and there are organisations that support human rights and protect user privacy on the Internet through free software and open networks. It is commonly said that anonymity on the Internet is ensured. The pursuit of anonymisation on the Internet and the constantly developing devices that improve navigation in the cyberspace show that this space exposes confidentiality to possible violations more than traditional ones. The desire for anonymity is associated with a sense of threat that may arise from using the Internet and transmitting data. There are many ways to remain anonymous online, but the possible attacks and their types are perhaps too numerous to list, as new technology continues to surprise as they improve hackers' possibilities and the latter enhance their skills.

The most popular attacks that can de-anonymise our network connection include those described herein: (a) browser attacks, such as those that force a TOR browser to unblock and provide information about the computer and the correct IP address; (b) node flooding, which involves the control of the network connection by the attacker, not by the client; (c) correlation attack, encompassing an flooding of large amounts of data coming in and out of the client's network. There are other possible attacks that are shown in the STRIDE model below.

Figure 3. STRIDE threat model[57]



57 Słota-Bohosiewicz, 2018, p. 300.

The STRIDE model is an acronym for: S, spoofing identity; T, tampering with data; R, repudiation; I, information disclosure; D, (ang.) denial of service; E, (ang.) elevation of privilege.[58]

The cyberspace is also a place where a new type of war is unfolding, often referred to as the information war. This type of warfare is defined as actions undertaken by one side to achieve information advantages, which in turn support the national military strategy by influencing the enemy's information and their information systems while protecting own information and information systems. These activities allow those involved to exert control over the content, flow, and availability of important information. There are two types of information warfare in the cyberspace, the first of which is (a) netwar, referring to a psychological warfare in the cyberspace, which provides propaganda aimed at shaping the morale of soldiers and society, and particularly at weakening the opponent's mental stability. It involves the integration of psychology, social communication, and modern information technologies. The second is (b) cyberwar, referring to activities carried out in the cyberspace to penetrate the enemy's infrastructure and then gain control over it or destroy it at the appropriate moment, while protecting own infrastructure. Nation states often hide their cyberspace activities under the guise of hacktivists, hackers, private armies, terrorist groups, and others. This is why they more often use the name cyberattack.

Importantly, there are threats of various sizes and levels of danger in the cyberspace, with some of the most dangerous ones being the following. First, cybercrime, referring to illegal, IT-based activities of non-state entities aimed at gaining profits. Second, cyber conflicts, describing conflicts related to cyberspace activities, which can generally be divided into activism (i.e. non-destructive activity in the cyberspace used to support different campaigns) and hacktivism (i.e. a combination of activism and criminal activities through the use of hacking methods against specific targets on the Internet to disrupt their functioning without causing serious losses). The latter is aimed not so much at destroying the opponent's resources but rather at drawing attention to a given problem. Third, cyberterrorism, describing politically-motivated attacks or threats of attacks on computers, networks, or information systems in order to destroy infrastructure and intimidate or force governments and the public to carry out far-reaching political and social actions in the broader sense of the word. It also involves the use of the cyberspace for communication, propaganda, and disinformation by terrorist organisations. Fourth, cyber espionage, referring to the use of the cyberspace for intelligence purposes, such as for obtaining information by bypassing or weakening systems, accessing the control mechanisms of hardware and software, and hacking into protected systems. Fifth, cyber surveillance, which is the control of society through information and communication technology (ICT) tools, and is most often used in authoritarian and totalitarian states. This is a phenomenon very similar to cyberterrorism, and may involve limiting citizens' access to the cyberspace.

58 Słota-Bohosiewicz, 2018, p. 299.

7. EU's actions in counteracting cyber incidents

7.1. EU institutions

The dynamic developments of and in the cyberspace have been forcing us to make great efforts at upholding security in this space at appropriate levels. Owing to the delineations above, the European Commission is taking actions aimed at establishing a close cooperation between EU countries and those that emphasise the role of the EU in ensuring network security. It is also making efforts to have this area recognised under EU policies. Over the years, as the cyberspace developed, several directorates have been established to deal with the issue of cybersecurity. These are the following: first, the Directorate-General for Communications Networks, Content and Technology (DG CNECT), the directorate responsible for shaping EU policy in the areas of electronic communications, digital content, technological innovation and, in general, the development of ICT. The main areas covered by the directorate are communication networks, digital content, digital technologies, and innovation and research.[59] Second, DG HOME (Cybercrime), responsible for the Digital Single Market and Security Union.[60] Third, the Directorate-General for Informatics (DG DIGIT), responsible for the IT management of EU institutions and supporting the development and implementation of IT technologies aimed at supporting the objectives of public administration and digital transformation. Its main activity areas are IT management, cybersecurity, digital transformation, support for technological innovations, and IT services.[61]

The implementation of these various tasks and responsibilities requires the support of various agencies in the EU, which include those described hereinafter: (a) ENISA, (b) European Cybercrime Center (also known as EC3), (c) European Union Computer Emergency Response Team (also known as CERT-EU), (d) European External Action Service (also known as EEAS). They also played important roles in the context of EU Member States and private sector organisations.

The ENISA, established in 2004 and headquartered in Heraklion, Crete, Greece, is responsible for upholding the highest level of security in the cyberspace in Europe. It serves as an advisory body in the field of network and information security, with its main goals being supporting EU Member States in the following: developing and implementing network and ICT security strategies; threat analysis; best practices promotion; education in the field of cybersecurity; international cooperation aimed at exchanging information and experiences; support in crisis situations related to information security.[62] The ENISA plays a key role in coordinating cybersecurity activ-

59 *Communications Networks, Content and Technology*, no date.
60 *Migration and home affairs*, no date.
61 *Digital Services*, no date.
62 *European Union Agency for Cybersecurity (ENISA)*, no date.

ities at the EU level, contributing to improvements to the cyber defence, along with the stability, of networks and information in territories of the EU and its Member States.[63]

The European Cybercrime Center, established in 2013 and based in the Hague, the Netherlands, is a unit of the European Law Enforcement Agency (also known as Europol) established to combat and prevent cybercrime. Its main tasks coordinating EU Member State activities, developing cooperation among law enforcement agencies and the private and public sectors, cooperating with relevant bodies in operational and investigative work, analysing and distributing information on the evolution of cyber threats, and conducting educational campaigns aimed at raising awareness of cyberattacks. As a key body of the EU strategy to combat cyber threats, it undertakes previously planned operational actions aimed at preventing cyberattacks,[64] as well as operational, analytical, and educational tasks.

The European Union Computer Emergency Response Team, established in 2011, is part of the ENISA and aims at preventing and responding to cyberattacks, as well as developing cybersecurity resources at the EU level. Its main tasks are responding analysing and responding to cybersecurity incidents, coordinating response activities among EU institutions and bodies, and providing technical and advisory support to EU Member States.[65]

The European External Action Service, established in 2010 under the Treaty of Lisbon, it is an institution responsible for managing and supporting the EU's foreign and security policies. Its main tasks are coordinating EU external activities, managing EU civil and military missions and operations as part of crisis management operations, peacekeeping, humanitarian aid, managing EU diplomacy and representation, providing support for political plans, analysing the international situation, cooperating with international partners.[66] This body has a unique entity status, combining elements of the European Commission and the Council of the European Union.

EU Member States are obliged to ensure their own cybersecurity and their activities in relation to EU policy should be carried out through the Council, within which there are numerous bodies coordinating activities and sharing information, such as the Horizontal Working Group on Cyberspace.

Private sector organisations encompass industry entities, Internet managers, and academia, serving as partners in relevant activities and influencing the creation and implementation of policies through contractual public–private partnerships.

63 Based on Lessmann et al., 2017.

64 *European Cybercrime Centre -EC3*, no date.

65 *CERT-EU*, no date.

66 European Union External Action – The Diplomatic Service of the European Union. [Online]. Available at: https://www.eeas.europa.eu/_en (Accessed: 10 January 2024).

7.2. Schedule of cybersecurity actions

The EU has been taking various actions to promote its resilience in the cyberspace and defence against cyber incidents, some of which are described in this subsection.[67] The first related activities took place on 9 June 2016, when the Council of the European Union started to work on improving the criminal justice system within the context of the cyberspace, specifically in relation to bilateral legal assistance, more effective cooperation with service providers, and factors determining jurisdiction. In addition, the Council addressed the need to improve the European Judicial Network on Cybercrime, endeavouring to strengthen the network of judicial authorities and increase the number of cybersecurity experts. The next important activity was the agreement on 24 October 2017, named the Cybersecurity Action Plan and the European Union Cybersecurity Reform Decision, which decided the nature of Internet security for the public and private sectors. Two months later, on 20 December 2017, close cooperation was established between EU entities in the fight against cyberattacks, and there was a decision to establish a Computer Emergency Response Team for all EU institutions, bodies, and agencies. This Team was aimed at coordinating the actions of EU institutions in response to cyberattacks on EU entities.

In 2018, various actions were taken to promote cybersecurity. In 16 April 2018, the Council adopted conclusions on the damages caused by cyberattacks, pointing to the essence of the cyberspace – which is supposed to be a global, free, and stable space wherein human rights and freedoms are respected – and also raised the issue of growing the cyberspace capabilities of non-EU countries and non-state entities. In 13 September 2018, the Council entered into negotiations with the European Parliament regarding the need to reach an agreement on the Cybersecurity Act, which was intended to increase the EU's cyber resilience by creating an EU-wide certification framework for ICT products, services, and processes. They also agreed on the modernisation of the ENISA, which was functioning at that time. In October 2018, the Council called for strengthening cybersecurity in the EU, and discussed the issue of intensifying preventive and response activities to emerging threats online, as well as hybrid, chemical, biological, radiological and nuclear threats. This was especially related to the cyberattacks carried out against the Organization for the Prohibition of Chemical Weapons in The Hague, the Netherlands. Finally, in December 2018, the Embassy of the European Union approved the Cybersecurity Act, which enabled the creation of EU-wide certification and strengthened the ENISA. As a result, devices connected to the Internet have been covered by EU-wide cybersecurity certifications.

In March 2019, the Council started negotiations with the Parliament on ways to consolidate knowledge on cybersecurity, and the European Cybersecurity Research and Competence Center was established, constituting a top-level knowledge base. A month later, the Council adopted the Cybersecurity Act, which established the

67 European Court of Auditors, 2019.

certification system in the EU and the European Union Agency for Cybersecurity. In May 2019, the Council was granted the power to impose sanctions to prevent and respond to cyberattacks, as such attacks were considered to constitute an external threat to EU Member States. Specifically, it was allowed to impose sanctions on entities and individuals who have done the following: (a) have carried out or attempted to commit a cyberattack; (b) supported these individuals financially, technically, and/or materially; (c) are directly involved in the attack at every stage of its preparation. To achieve common foreign and security policy objectives, these regulations were made applicable to non-EU entities or countries, as well as to international organisations targeting cyberattacks. On 3 December 2019, an important event discussed the importance of the 5G network for the European economy and the risks associated with it.

On 5 June 2020, the need to negotiate a European regulation on the Cybersecurity Competence Center and the Network of National Coordination Centers I for the development of the 5G network was established. A month later, on 9 June 2020, the Council took steps to implement the EU digital strategy, highlighting that the scale and complexity of cybersecurity threats was increasing, along with the need to improve the EU's response to cyberattacks. The first sanctions for carrying out cyberattacks were imposed on six people and three entities on 30 July 2020, involving the above-mentioned travel ban and asset freeze sanctions. On 2 December 2020, the Council highlighted various new risks arising from connecting many office and home devices to the Internet, and emphasised that these are new threats to sensitive private and public data. On 9 December 2020, the European Center for Cybersecurity in Industry, Technology and Research in Bucharest was provided with the task of coordinating research and innovation in the field of cybersecurity in the EU, and combining cybersecurity investments with research, technology, and industrial development. Three days later, on 11 December 2020, talks began about establishing an EU Cybersecurity Competence Center. Thereafter, on 15 December 2020, the Council pointed to the need to strengthen resilience and counteract hybrid threats, including disinformation. It prepared a statement in the context of the COVID-19 pandemic as well as various other crises, and emphasised the need to develop a comprehensive approach that will define the principles of coordination and cooperation for counteracting threats and disinformation on the Internet.

In 2021, some issues related to the EU's cybersecurity strategy were raised, with much attention paid to citizens and businesses in the context of their protection against cyber threats. Issues of promoting the security of IT systems and global protection, as well as a safe cyberspace, were also discussed, and it was stressed that cybersecurity is crucial for Europe, which must be resilient, green, and digital. On 22 March 2021, the importance of the EU in achieving leadership in the digital realm and defining its strategic capabilities was discussed. A month later, on 20 April 2021, the European Center for Industrial, Technological and Research Competences in the field of cybersecurity was established, being tasked

to cooperate with a network of designated national centres to increase Internet security. An interim agreement was also reached, on 29 April 2021, to enable ISPs to continue to detect, remove, and report online child sexual exploitation. This year, there were also the following processes: (a) extension of sanctions for cyberattacks against EU countries (from 17 May 2021 to 18 May 2022); (b) the Council maintained its position on the need to develop initiatives regarding crisis management in cyberspace (19 October 2021); (c) the Council agreed to develop a new cybersecurity directive (13 December 2021).

In 2022, the EU Ministers emphasised the need to intensify European cooperation in the area of cybersecurity, especially after the various cyber threats that emerged owing to the situation in Ukraine, and, consequently, by the increase in the number of cyber incidents in the EU. As a result, between 8 and 9 March 2022, 27 ministers adopted a political declaration aimed at strengthening the EU's cybersecurity capabilities. In addition, the Council and the European Parliament made efforts to create the Digital Operational Resilience Regulation (DORA), which provides a technical framework to enable all companies to achieve the goal of strengthened cybersecurity. On 11 May 2022, special procedures were included in the regulation with the aim of preventing ICT disruptions, and temporary terms of agreement were set on the proposed NIS2 Directive, which was to replace the Directive on the security of network and information systems (NIS). The main goal was to achieve the highest level of cybersecurity in all EU countries (13 May 2022). The Council's actions were also important during this period, and encompassed the following: (a) the Council extended the rules regarding sanctions (16 May 2022) and approved (23 May 2022) the principles and policies of the EU, as well as the EU plan, to strengthen security and defence policies (Strategic Compass) by the end of 2030; (b) adopted Sorava's conclusions on a coordinated EU response to hybrid campaigns (21 June 2022); (c) accepted conclusions on ICT supply chain security (17 October 2022); (d) defined a common cybersecurity policy and the EU actors responsible for security (11 November 2022); (e) adopted the NIS2 directive (28 November 2022).

In 2023, the Council adopted the following: (a) conclusions on cyber defence, emphasising that each EU country has the obligation to further strengthen its own resilience to cyberattacks while enhancing its cybersecurity and cyber defence (23 May 2023); (b) an interim agreement with security entities on a common cybersecurity framework for EU entities (26 June 2023); (c) a common position on the Cyber Resilience Act (19 July 2023); (d) updated the policy framework, which now includes efforts at increasing the resilience to cyberattacks, the intensity of cooperation between EU Member States, and the ability to defend against cyberattacks (19 November 2023). The evolution of the security challenges was also analysed, and the competences of various EU entities were defined in the year of 2023. There were also discussions involving the need to build strong EU cybersecurity and the need to define sanctions for the use of cyberattacks.

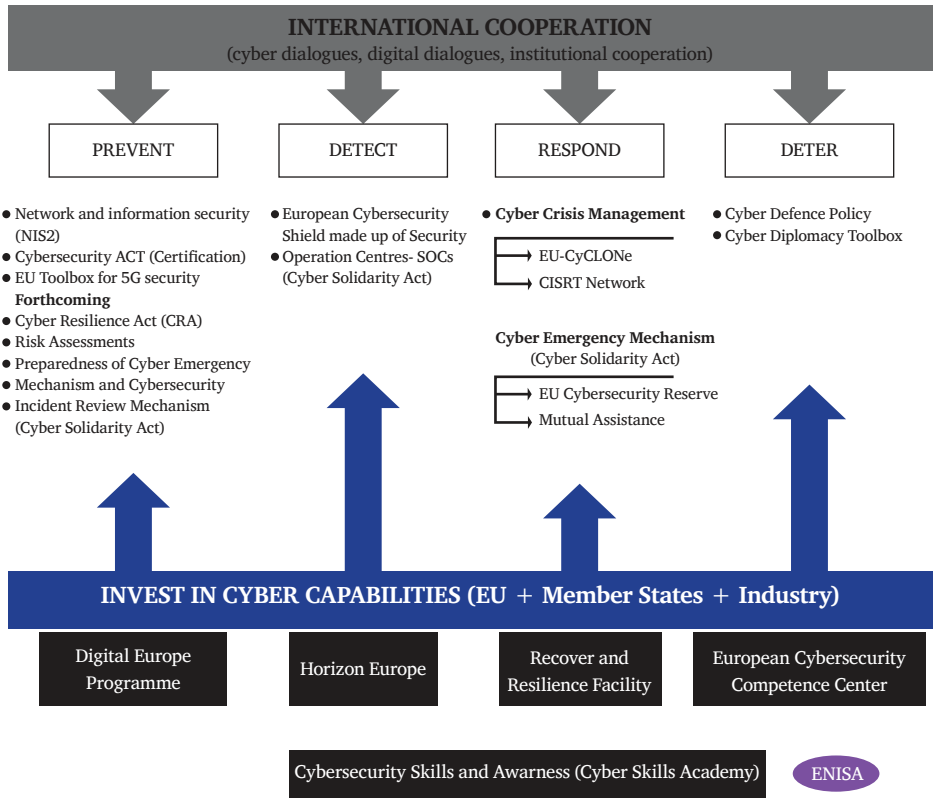
7.3. International cooperation

The EU has taken many actions to ensure security in the cyberspace, one of which is the EU Cybersecurity Strategy, which assumes actions aimed at increasing the EU's ability to fight against cyberattacks and effectively and quickly recover from related attacks. The cyberspace enables many activities that can be both beneficial and downright dangerous for nations, and the cyberattacks that are becoming the most common are those aimed at stealing data and spying on users or government data; that is, attacks targeting both the private and public sectors.[68] This underpins the importance of securing the safe use of the network by all sectors.

The EU Cybersecurity Strategy aims to strengthen the EU's common cybersecurity and its response to cyberattacks. It is also important that human rights and the rule of law are protected, and to safeguard these principles, the strategy has been divided into the following areas:[69] (a) resilience, technological sovereignty, and leadership; (b) operational capability to prevent, deter, and respond; (c) cooperation for the development of a global and open cyberspace. Cybersecurity has been included in the "Digital Europe" program, which aims to strengthen the coordination of cybersecurity among EU Member States, and finance the maintenance of their resilience to cyberattacks. Research is constantly being carried out to improve the existing EU strategies and policies, and the main goal is to improve the cooperation and investment in cyber defence in order to provide better protection against the increasing number of cyberattacks.[70] Achieving these goals will surely require EU Member States to cooperate in preventing, detecting, and responding to cyber threats as well as improving cyber security. These goals are presented in detail in the diagram below.

68 European Court of Auditors, 2019, pp. 13–16.
69 Based on International Civil Aviation Organization, 2022.
70 *Cyberbezpieczeństwo* [Cybersecurity], no date.

Scheme 1. International cooperation



The diagram provides an overview of the EU's work on various fronts to promote its cyber resilience, safeguarding its online society, communication, data, and economy.

8. Responding to cyber incidents and cyberattacks: Good practices

8.1. Sectors and groups at risk

Nowadays, in the era of digitalisation and ubiquitous threats in the cyberspace, everyone, from citizens, their families, and large groups, should be ready to respond to online incidents. Statistics show that individuals, large corporations, and

government entities are all attacked, showcasing that cyber threats pose a real risk to enterprises, public institutions, non-profit organisations, and other entities. More specifically, some groups that are particularly vulnerable to these threats include those outlined herein: (a) business sector (e.g. business organisations, small and medium-sized enterprises); (b) financial sector (e.g. banks, financial institutions, financial services companies); (c) government sector (e.g. possible loss of sensitive data regarding personnel and citizens, which may lead to disruption of state functioning stability); (d) health sector (possibility of losing patient data, which may have serious consequences for patient safety); (e) energy sector (possibility of disruption of energy supplies); (f) manufacturing sector; (g) infrastructure sector; (h) education sector (possible loss of student and teacher data and possible disruptions in the educational system); (i) non-profit sector (possibility of losing data of sponsors and sponsored persons, along with the disruption of social, humanitarian, and charitable assistance activities); (j) cloud and IT service provider sector (disruption in the supply of services may disrupt the functioning of the organisation and disrupt the lives of citizens); (k) civil society (individual users and corporate employees); (l) security teams; (m) crisis management teams; (n) incident response teams; (o) management of boards of directors.

Good practices for dealing with a cyber incident should include several stages, as follows: defining who is at risk; taking actions to prevent cyber incidents; preparing for cyber incidents, responding to the incidents (incident management); restoring the state to normal after the cyber incident has been removed.

8.2. Prevention[71]

The first stage is incident prevention, which is a strategic stage of an effective cyber security plan. The related procedures at this stage include those outlined herein: (a) raising awareness and education about cyber threats (e.g. through regular training and information campaigns); (b) implementing safety rules (e.g. applies to management, executive staff, teachers, children); (c) using security measures (e.g. strong passwords, frequently changing passwords, creating access restrictions, prohibiting the use of unregistered devices, and media); (d) software updates (especially applicable to operating systems and applications); (e) using technical security measures (e.g. firewalls, anti-virus systems, and protection against ransomware); (f) controlling access (e.g. through creating permissions and access restrictions); (g) security monitoring (e.g. using systems that detect inappropriate behaviour); (h) developing a policy for the use of IT systems; (i) monitoring employee activities; (j) establishing network security; (k) creating protections against phishing; (l) managing system and application configurations; (m) exchanging information with entities about threats; (n) conducting external security audits.

71 Based on International Civil Aviation Organization, 2022.

8.3. Preparation[72]

The preparation stage for cyberattacks includes activities such as those presented in the list that follows: (a) developing an incident management plan comprising[73] the definition of procedures and stages of response to various events, role divisions, competences, and responsibilities between responsible entities; (b) establishing an incident team (i.e. the Computer Security Incident Response Team, also known as CSIRT); (c) participating in training and exercises in the context of cyber threats; (d) implementing monitoring and detection systems; (e) implementing access management systems; (f) applying technical security measures; (g) developing recovery plans; (h) regularly conducting external security audits; (i) applying legal plans; (j) promoting external cooperation with law enforcement agencies, cybersecurity organisations, and other industry organisations to exchange information and best practices about cybersecurity organisations and others.

8.4. Response/incident management[74]

The response stage for cyberattacks includes activities such as the following: (a) recognising incidents, which is carried out by system monitoring (i.e. early detection of incidents), analysing event logs, reporting suspicious activity by staff, reporting of suspicious activities by automatic threat detection systems; (b) classifying and assessing the incident, which is carried out by identifying the nature and scale of the event, as well as analysing and assessing potential impacts on the organisation (e.g. financial damage, data loss, impact on reputation, and operational functioning); (c) isolating resources affected and taking immediate actions to thwart the spread of an attack; (d) notifying appropriate teams (e.g. IT Security Team, the Computer Security Incident Response Team, Crisis Management Team, relevant internal teams); (f) managing the Computer Security Incident Response Team; (g) collecting data to be analysed and documented afterwards; (h) conducting incident analysis; (i) notifying appropriate external parties (e.g. law enforcement agencies, international structures, partner institutions, among others); (j) restoring services and systems and verifying that the corrective steps taken are effective and safe; (k) analysing post-event conclusions and introducing changes to the strategy and security measures, as well as improvement activities; (l) implementing training and education through developing and disseminating educational materials, and using experience to increase the ability to counteract incidents; (m) reporting and documentation covering the scope of activities, conclusions, and recommendations.

72 Based on International Civil Aviation Organization, 2022.
73 Based on International Civil Aviation Organization, 2022.
74 *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* [Procedure manual with incidents of violation computer security], 2021.

8.5. Reconstruction[75]

The reconstruction stage comes after the end of an incident and is of particular importance for dealing with cyberattacks. This is because the efforts of many entities must be coordinated to ensure a successful restoration of the status to that before the occurrence of the cyberattack. It comprises activities such as the following: (a) conducting loss analysis; (b) analysing the causes of the incident; (c) strengthening security; (d) promoting staff education; (e) increasing awareness of the public and staff; (f) applying internal and external information policy; (g) making efforts to secure system recovery; (h) resting the services; (i) verifying the effectiveness of actions taken so far; (j) updating system patches; (k) reviewing and updating plans; (l) verifying procedures; (m) improving procedures; (n) tightening cooperation with external entities; (o) promoting information exchanges.

9. Summary

The analysis of the literature on the subject, reports, internet sources, and of research conducted with experts allows the conclusion that the cyberspace has become important in almost all sectors of life. It is a dimension of life that allows us to take actions that can bring both benefits and losses and stores a very large amount of information, including sensitive information, which can be stolen and used and may cause financial and health losses. Cyberattacks can thus contribute to causing crises, panic in society, chaos, tension, unrest, and even war, and these attacks seems to also be getting more complex and aggressive as time goes on. It is very important for the whole society, as well as private and government organisations, to be aware of cyberattacks and to be able to respond to them. Effective cyberattack detection and response is now becoming a challenge for countries worldwide, especially as cross-border attacks become particularly important and require coordination of the EU crisis response mechanism. In light of these complex scenarios, it is key that the EU makes grand efforts to protect its critical infrastructure, but achieving these goals, if we consider the current challenges in the network, may require the involvement of all EU Member States.

75 Based on International Civil Aviation Organization, 2022.

References

Barć, M. (2021) 'Rodzaje Ochrony Infrastruktury Krytycznej' [Types of infrastructure protection], *Rocznik Bezpieczeństwa Morskiego*, special issue, pp. 1–15; https://doi.org/10.5604/01.3001.0015.0196.

Cendrowski, W. (2020) 'Cyberbezpieczeństwo' [Cybersecurity], *UKEN: Vademecum Bezpieczeństwa Informacyjnego*, 9 March 2020. [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/09/cyberbezpieczenstwo/ (Accessed: 6 January 2024).

Czekaj, Ł. (2020) 'Cyberatak' [Cyber attack], *UKEN: Vademecum Bezpieczeństwa Informacyjnego*, 9 March 2020. [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/09/cyberatak/https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/09/cyberatak/ (Accessed: 10 January 2024).

Encyclopedia by Kaspersky (no date). [Online]. Available at: https://encyclopedia.kaspersky.com/knowledge/years-1970s/ (Accessed: 8 November 2023).

European Court of Auditors (2019) 'Challenges to effective EU cybersecurity policy', *Briefing Paper*, March 2019. [Online]. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (Accessed: 10 January 2024).

European Union Agency for Cybersecurity (2020a) *Zagrożenia Wewnętrzne: Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa* [Internal Threats: Threat Landscape according to the European Union Agency for Cybersecurity]. [Online]. Available at: https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-insider-threat-ebook-en-pl.pdf (Accessed: 20 November 2023).

European Union Agency for Cybersecurity (2020b) *Wykaz piętnastu największych zagrożeń* [The list of fifteen of the largest threats]. [Online]. Available at: https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-enisa-list-of-top-15-threats-ebook-en-pl.pdf (Accessed: 5 January 2024).

European Union Agency for Cybersecurity (2021) *Krajobraz Zagrożeń 2021 wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)* [Threats Landscape 2021 According To European Union Agency For Cyber Security (ENISA)], October 2021. [Online]. Available at: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_pl.pdf (Accessed: 6 January 2024).

Falliere, N., O Murchu, L., Chien, E. (2010) *W32.Stuxnet Dossier*, November 2010. [Online]. Available at: https://web.archive.org/web/20191104195500/https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf (Accessed: 2 January 2024).

Gopal, R.V. (2022) 'Complete Case Study – Target Data Breach', *Medium*, 4 December 2022. [Online]. Available at: https://medium.com/@rithikvgopal/complete-case-study-target-data-breach-2-ba4bb365a82e (Accessed: 2 January 2024).

Grzelak, M., Liedel, K. (2012) 'Bezpieczeństwo w Cyberprzestrzeni. Zagrożenia i Wyzwania dla Polski – zarys problemu' [Security in cyberspace. Threats and challenges for Poland – outline of the problem], *Bezpieczeństwo Narodowe*, 22(2), pp. 125–139.

International Civil Aviation Organization (2022) *Cybersecurity Action Plan*, January 2022. [Online]. Available at: https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf (Accessed: 10 December 2023).

Lessmann, F. et al. (2017) 'Study on the Evaluation of the European Union Agency for Network and Information Security, European Comission', *European Commission: Directorate-General for Communications Networks, Content and Technology*. [Online]. Available at: https://op.europa.eu/en/publication-detail/-/publication/ed504f6e-9c1c-11e7-b92d-01aa75ed71a1/language-en (Accessed: 10 January 2024).

Liderman, K. (2020) 'Ochrona informacji sterującej w sieciach i systemach przemysłowych – propozycja podstaw edukacyjnych' [Protection of control information in industrial networks and systems – a proposal for educational foundations], *Przegląd Teleinformatyczny*, 8(26), pp. 3–30; https://doi.org/10.5604/01.3001.0015.0604.

Marczyk, M. (2018) 'Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa' [Cyberspace as a new dimension of human activity – conceptual analysis of the area], *Przegląd Teleinformatyczny*, 6(24), pp. 59–72; https://doi.org/10.5604/01.3001.0012.7212.

Niewiadomska-Szynkiewicz, E., Litka, R. (2023) 'Ataki na urządzenia mobilne I metody ich wykrywania' [Attacks on mobile devices and methods of detecting them], *Cybersecurity and Law*, 1(9), pp. 95–107; https://doi.org/10.35467/cal/169303.

Nowak-Brzezińska, A. (2017) *Zagrożenia i bezpieczeństwo komputerów i danych* [Threats and security of computers and data]. Warsaw: Projekt UPGOW, European Social Fund.

Oladimeji, S., Kerner, S.M. (2023) 'SolarWinds hack explained: Everything you need to know', *TechTarget*, 3 November 2023. [Online]. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (Accessed: 20 December 2023).

Pacut, M. (2023) 'Co to jest naruszenie bezpieczeństwa danych (data breach)?' [What is a data breach?], *Net Complex Blog*, 28 April 2023. [Online]. Available at: https://www.netcomplex.pl/blog/co-to-jest-naruszenie-bezpieczenstwa-danych-data-breach (Accessed: 20 November 2023).

Pala, M. (2015) 'Wybrane aspekty bezpieczeństwa w cyberprzestreni' [Selected aspects of security in cyberspace], *De Securitate et Defensione. O bezpieczeństwie i Obronności*, 1(1), pp. 113–130.

Petrosyan, A. (2024) 'Annual number of malware attacks worldwide from 2015 to 2022 (in billions)', *Statista*, 22 April 2024. [Online]. Available at: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/ (Accessed: 10 April 2024).

Sarkar, D. (2023) 'Elk Cloner – The First Computer Virus', *Linkedin*, 26 July 2023. [Online]. Available at: https://www.linkedin.com/pulse/elk-cloner-first-computer-virus-debadrita-sarkar (Accessed: 11 January 2024)

Słota-Bohosiewicz, A. (2018) 'Przeciwdziałanie cyberszpiegostwu w organizacji' [Counteracting cyber espionage in an organization], *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej*, 4(28), pp. 294–312.

Thomson, I., Nichols, S. (2009) 'Top ten worst viruses', *PC & Tech Authority*, 4 May 2009. [Online]. Available at: http://web.archive.org/web/20180614194509/https://www.pcauthority.com.au/news/top-ten-worst-viruses-143993 (Accessed: 8 November 2023).

Waraksa, M., Żurek, J., Niski, R. (2011) 'Interfejsy radiowe w bezprzewodowych sieciach sensorowych' [Security of data transmission in wireless sensor networks], *Zeszyty Naukowe Akademii Morskiej w Gdyni*, 2011/70, pp. 79–87.

Wasiuta, O., Klepk, R. (eds.) (2019) *Information security handbook*. Kraków: AT Wydawnictwo- LIBRON, Uniwersytet Pedagogiczny.

Zhu, L., Zheng, B., Shen, M., Yu, S., Gao, F., Li, H., Shi, K., Gai, K. (2018) 'Research on the Security of Blockchain Data: A Survey', *Journal of Computer Science and Technology*, 35(4), pp. 843–862; https://doi.org/10.48550/arXiv.1812.02009I.

I 10 virus informatici peggiori della storia [The 10 Worst Computer Viruses in History] (no date) *Hardware Upgrade*. [Online]. Available at: https://www.hwupgrade.it/forum/showthread.php?t=1978965 (Accessed: 10 February 2024).

Ataki na aplikacje webowe. Jakie są najczęstsze i jak się bronić? [Attacks on web applications. What are the most common ones and how to defend yourself?] (2022) *Da Vinci Studio*, 26 October 2022. [Online]. Available at: https://www.davinci-studio.com/pl/blog/ataki-na-aplikacje-webowe-jakie-sa-najczestsze-i-jak-sie-bronic/ (Accessed: 22 January 2024).

Analiza ryzyka w obszarze cyberbezpieczeństwa – jakie jest jej znaczenie? [Risk analysis in the area of cybersecurity – what is its importance?] (no date) *Szkoła Biznesu Politechniki Warszawskiej*. [Online]. Available at: https://biznes.edu.pl/analiza-ryzyka-w-obszarze-cyberbezpieczenstwa-jakie-jest-jej-znaczenie/ (Accessed: 13 January 2024).

ABlockchain – aspekty technnologiczne oraz przykłady zastowań [Blockchain – technological aspects and examples of applications] (no date) *Lazarski University*. [Online]. Available at: https://www.lazarski.pl/pl/34024-blockchain-aspekty-technologiczne-oraz-przyklady-zastosowan (Accessed: 20 November 2023).

Celebrating Penn Engineering History: ENIAC (no date) *University of Pennsylvania*. [Online]. Available at: https://www.seas.upenn.edu/about/history-heritage/eniac/ (Accessed: 3 November 2023).

CERT-EU (no date) *Cyber security intelligence*. [Online]. Available at: https://www.cybersecurityintelligence.com/cert-eu-1925.html (Accessed: 10 January 2024).

Communications Networks, Content and Technology (no date) *European Commission*. [Online]. Available at: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/communications-networks-content-and-technology_en (Accessed: 10 January 2024).

Cyberbezpieczeństwo [Cybersecurity] (no date) *European Commission*. [Online]. Available at: https://digital-strategy.ec.europa.eu/pl/policies/cybersecurity (Accessed: 10 January 2024).

Cyberbezpieczeństwo: główne i nowe zagrożenia [Cybersecurity: main and new threats] (2022) *European Parliament*, 27 January 2022. [Online]. Available at: https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia#ssh_slides (Accessed: 30 November 2023).

Cybersecurity: how the EU tackles cyber threats (no date) *European Council*. [Online]. Available at: https://www.consilium.europa.eu/en/policies/cybersecurity/ (Accessed: 10 November 2023).

Czym jest uwierzytelnianie dwuskładnikowe, uwierzytelnianie dwuetapowe? [What is two-factor authentication, two-step authentication?] (2023) *Progreso*, 18 September 2023. [Online]. Available at: https://progreso.pl/pl/blog/czym-jest-uwierzytelnianie-dwuskladnikowe-uwierzytelnianie-dwuetapowe (Accessed: 20 November 2023).

Digital Services (no data) *European Commission*. [Online]. Available at: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/digital-services_pl (Accessed: 10 January 2024).

Elk Cloner. La cápsula del tiempo [Elk Cloner. The Time Capsule] (2009) *WeLiveSecurity*, 11 August 2009. [Online]. Available at: https://www.welivesecurity.com/laes/2009/08/11/elk-cloner-capsula-tiempo/ (Accessed: 11 January 2024).

European Cybercrime Centre -EC3 (no date) *Europol*. [Online]. Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Accessed: 10 January 2024).

European Union Agency for Cybersecurity (ENISA) (no date) [Online]. Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_pl (Accessed: 10 January 2024).

Incydent bezpieczeństwa informacji – kiedy następuje? **[**Information security incident – when does it occur and what to do?] (2024) *Ce cert*, 7 June 2024. [Online]. Available at: https://cecert.pl/incydent-bezpieczenstwa-informacji-kiedy-nastepuje-i-jak-wtedy-postepowac/ (Accessed: 10 February 2024).

Internet Rzeczy, ochrona prywatności a bezpieczeństwo danych [Internet of Things, privacy protection and data security] (2021) *Deloitt*e, 8 February 2021. [Online]. Available at: https://lgl-iplaw.pl/2021/02/internet-rzeczy-iot-internet-of-things-wygoda-czy-prawo-do-prywatnosci-wirtualnej-i-cyberbezpieczenstwo/ (Accessed: 20 November 2023).

A look at Estonia's cyberattack in 2007 (2009) *NBC News*, 8 July 2009. [Online]. Available at: https://www.nbcnews.com/id/wbna31801246 (Accessed: 2 January 2024).

Microsoft Faces Blistering Attack On-Line Leaders Say Software Giant Wants To Extend Its Dominance (1995) *The Spokesman–Review*, 20 July 1995. [Online]. Available at: https://www.spokesman.com/stories/1995/jul/20/microsoft-faces-blistering-attack-on-line-leaders/ (Accessed: 2 January 2024).

Migration and home affairs (no date) *European Commission*. [Online]. Available at: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/migration-and-home-affairs_en (Accessed: 10 January 2024).

The Morris Worm: 30 Years Since First Major Attack on the Internet (2018) *FBI*, 2 November 2018. [Online]. Available at: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218 (Accessed: 2 January 2024).

Naruszenie ochrony danych przez podmiot przetwarzający. Czym jest i jak postępować, kiedy do niego dojdzie [Data protection breach by the processor. What is it and what to do when it happens] (2021) *Polska Agencja Rozwoju Przedsiębiorczości*, 8 July 2021. [Online]. Available at: https://www.parp.gov.pl/component/content/article/72064:naruszenie-ochrony-danych-przez-podmiot-przetwarzajacy-czym-jest-i-jak-postepowac-kiedy-do-niego-dojdzie (Accessed: 20 November 2023).

Phishing: co to jest? [What is phishing?] (no date) *Trend Micro*. [Online]. Available at: https://www.trendmicro.com/pl_pl/what-is/phishing.html (Accessed: 20 November 2023).

Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego [Procedure manual with incidents of violation computer security] (2021) *Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa*, Warszawa, 2021. [Online]. Available at: https://www.gov.pl/web/baza-wiedzy/podrecznik-postepowania-z-incydentami-naruszenia-bezpieczenstwa-komputerowego (Accessed at: 10 December 2021).

Poradnik ransomware [Guide Ransomware] (no date) *CERT Polska*. [Online]. Available at: https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf (Accessed: 22 January 2024).

SMEs and Cybercrime (2022) *European Commission*, May 2022. [Online]. Available at: https://europa.eu/eurobarometer/surveys/detail/2280 (Accessed: 10 February 2024).

Triada CIA – Podstawowe Spojrzenie Na Bezpieczeństwo Informacji [The CIA Triad – A Basic View of Information Security] (2021) *Security bez tabu*, 15 July 2021. [Online]. Available at: https://securitybeztabu.pl/triada-cia-podstawy-bezpieczenstwa/ (Accessed: 22 January 2024).

What is WannaCry ransomware? (no date) *Kaspersky*. [Online]. Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (Accessed: 20 December 2023).

Y2K bug (no date) *National Geographic*. [Online]. Available at: https://education.nationalgeographic.org/resource/Y2K-bug/ (Accessed: 2 January 2024).

Chapter 15

Legal Aspects of Cyberwarfare and Cyberwarfare Crimes: Criminal Law Analysis and Dilemmas in the Legal System of the European Union

Miha Šepec

Abstract

The goal of this chapter is to analyse the substantive legal content regarding cyberwarfare attacks and crimes, present procedural measures of cooperation in criminal matters for the purpose of prosecuting such crimes, and examine European Union's (EU) institutions for cooperation in such criminal matters. It should be emphasised that cyberwarfare does not have a single, clearly established legal definition. In most cases, cyberwarfare attacks refer to forms of cyberattacks that are already known, and which most EU Member States have already defined as criminal acts. The specifics of cyberwarfare are, thus, that it is connected with the army of an individual country, which then configures a military operation; and that the range and scope of the offence are significantly wider, as cyberwarfare attacks focuses on more important targets with significantly more repulsive motives, such as paralysing a country's national security via attacks on its infrastructure and technological centres. The focus of the legal analysis is placed on the EU legislation and United Nations (UN) conventions, with particular interest on the legal definitions of terms connected to cyberwarfare (e.g. cyberattack, cyber espionage, and cyber-spying), understanding in which legal documents these terms are defined, and if these documents are legally binding to EU Member States. The study proves that cyberwarfare attacks are treated

Miha Šepec (2024) 'Legal Aspects of Cyberwarfare and Cyberwarfare Crimes: Criminal Law Analysis and Dilemmas in the Legal System of the European Union'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 663–697. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_15

in the EU as crimes with a cross-border dimension of such nature and impact that they need special treatment, that is, they require a harmonising legislation at the EU level to prosecute such crimes more efficiently.

Keywords: Cyberwarfare, Cyberattack, Defence Policy, Legal framework, Criminal Law, European Union

1. Introduction

We currently live in the digital age, where humanity is becoming increasingly dependent on electronic information systems that regulate and control most of the tasks we perform. Computer systems are increasingly penetrating society and replacing human work. In the future, information technology is likely to completely change the views we have on law and legal doctrines regarding the functioning of society. Specifically, the invention that may bring about a drastic change in society and law may be the speculated development of a self-aware artificial intelligence (AI). The term AI was developed in 1956 by the American scientist John McCarthy When describing the science of engineering of intelligent machines.[1]

Computer information systems, similar to any major human invention, also have disadvantages, the most noticeable of which is its excessive dependence on information technology. Along with such invention also came new forms of criminal acts committed with the help of these information systems. Criminal acts have existed in the cyberspace since the beginning of its development, and despite being initially relatively simple, they have been becoming increasingly complex and multifaceted. Today, we discuss topics related to a new form of crime that connects information systems, the cyberspace, and digital technology, and is called cybercrime. This type of crime includes all emergent forms of criminal acts studied within the framework of criminal law theory.

Cybercrime is considered the fastest growing criminal phenomenon in the current world. Therefore, criminal law must follow its rapid development and adapt to the specifics of prosecuting cybercrime offences. To define the new acts associated with cybercrime, we must first have detailed and accurate knowledge of the trends and forms of criminal behaviour in information systems. In general, criminal acts of cybercrime are divided into three large groups:

1. *integrity-related crimes*, where the information system is the target of the attack;
2. *computer-related crimes,* where the information system is used as a tool or accessory to commit a crime (e.g. computer fraud);

1 McCarthy, 1990, pp. 226–236.

3. *content-related crimes*, where crime is linked to a certain digital content (e.g. child pornography).[2]

The term cyberspace was first used in 1984 by Gibson in his book Neuromancer.[3] He used the term to refer to a space in which computer hackers engage in "war" to obtain confidential data that does not exist in the physical world. Thus, the cyberspace looks like the real world, but is actually a computer-generated construct of abstract data. In 2001, with the introduction of the Council of Europe's Convention on Cybercrime,[4] the term cybercrime was finally established internationally as a term that refers to all forms of criminal acts committed in the cyberspace, and it is a term commonly used today in established literature.[5]

For as long as the human race has existed, we have known war, and it is an undeniable part of our history. In fact, if we consider our historical past, there is space for arguing that it has often been the first, or sometimes the sole, way to resolve intercultural, interracial, and interstate conflicts. Furthermore, ever since its advent, the military industry has constantly developed new warfare methods using the latest technologies and means available to humans, and digital information technologies are no exception to this rule. Actually, the accelerated development of these technologies is often a reflection of the development of the war industry. It is also clear that the dimensions that new information technologies bring to the military industry are unimaginable. Today, cyberwars and/or information wars are major threats to countries worldwide, and in terms of definition, information warfare represents actions aimed at achieving information superiority by attacking a country's information centres thereby weakening it. Barrett explained that we can speak of information warfare only when actions are carried out within the framework of a national military strategy, and when both offensive and defensive actions are involved.[6] In 1997, the author predicted that, in the future, information armament in wars would reach the same status as the strength and number of classic military units.[7] Today, we can affirm that his predictions have proven almost entirely true. It is practically impossible to imagine a modern army without a strong information department, and a prime example is featured in the US Army and its special unit for this purpose, named the Cyber Command. This Command is dedicated exclusively to information warfare and defence.[8]

Digital warfare can be carried out between states, paramilitary units, or when states participate only indirectly (e.g. providing financial, legal, or moral support

2 Wall, 2005, pp. 77–98.
3 Gibson, 1984.
4 Council of Europe, 2001, CETS No. 185.
5 Clough, 2010, p. 9.
6 For example, the actions of a group of hackers who attack and weaken an important information centre of the country cannot be called an information war if the hackers are not operating under the auspices of the state or the military.
7 Barrett, 1997, p. 168.
8 Available at: https://www.arcyber.army.mil/ (Accessed: 30 August 2023).

to perpetrators who attack the basic infrastructure of a rival state). Barrett further distinguished between information warfare (i.e. involving attacks on military and operationally important targets) and full information warfare (i.e. involving attacks on strategically important state targets coordinated by top military and state officials).[9]

Cyberterrorism is relevant in today's era, as it involves the use of information networks to damage or destroy critical state infrastructures (e.g. energy structures, transportation systems, and state leadership establishments). In cyberterrorism, this is done for political, religious, or ideological reasons, and with the aim of instilling fear in the public and influencing the actions of state authorities.[10] Cybercrime and cyberterrorism are not synonymous, as attacks in the cyberspace must have a terrorist component to be considered cyberterrorism. Specifically, the attack must inspire fear and terror, which may result in death or destruction on a larger scale, and must have political motives. Terrorists also use computer systems as means for their activities, such as propaganda, recruitment, data collection, and communication.[11]

There is no single definition of cyberwarfare, but at its core, it means using computer technology to disrupt or destroy an adversary's information systems and networks. These are actions in cyberspace that threaten key state infrastructure systems in the form of armed conflicts with destructive effects. Attacks on state infrastructure can threaten or destroy the country's fundamental processes, paralyse the economy, and tarnish the country's reputation; the consequences are manifested in monetary damages as well as bodily harm or death of victims. Attacks on military networks threaten classified information and communication systems, as well as military operations. Moreover, espionage undermines national security during peacetime and wartime, while also enabling the theft of sensitive information.[12]

Today, cyberwarfare is present in practically every military operation, and classic military operations now customarily overlap with cyber operations. The enemy infrastructure can be destroyed with conventional weapons, but it can also be crippled or destroyed by cyberattacks. An example of such a cyberattack was the Stuxnet worm attack in 2010, which was directed against Iran's nuclear facilities, particularly its uranium enrichment centrifuges.[13] Stuxnet caused physical damage to Iran's nuclear infrastructure by manipulating its industrial control systems. In 2015 and 2016, Ukraine's power grids were also targets of cyberattacks,[14] causing widespread power outages, demonstrating that cyberwarfare can paralyse or at least disrupt critical services and infrastructure, and can have devastating consequences for countries and civilians.

9 Barrett, 1997, p. 170.
10 Clough, 2010, p. 12.
11 Wimann, 2005, p. 132.
12 Digmelashvili, 2023, pp. 12–19.
13 *Struxnet*, no date.
14 *Cyber-Attack Against Ukrainian Critical Infrastructure*, 2021.

Considering that technology is constantly developing, and that an ever-increasing part of the world depends on modern technologies, the potential for cyberwarfare is extremely large. In the future, European Union (EU) Member States will have to invest heavily in information technology, in addition to standard military equipment, and traditional soldiers will begin to be supplemented by information-aware soldiers, whose profiles will be completely different. Physical fitness and training will not play as much of a role as intelligence, computing and hacking skills, computer awareness, and the ability to manage advanced cyber operations. Thus, as the world changes, so do the methods of warfare, and the law must follow these changes and legally cover the new forms of warfare.

As expressed by Karim A. A. Khan, Prosecutor of the International Criminal Court:

> Cyber operations are sometimes employed as part of a so-called "hybrid" or "grey zone" strategy. Such strategies aim to exploit ambiguity and operate in the area between war and peace, legal and illegal, with the perpetrators often hidden behind proxy actors. This calls for a whole-of-society response, drawing together distinct functions and capabilities to act in a coordinated way.[15]

In this chapter, we provide a legal introduction to cyberwarfare and related crimes, presenting the definitions and legal meanings of cyberwarfare. We also list the legal acts at the EU and United Nations (UN) levels that deal with cyberwarfare and its crimes. Moreover, this section delves into the criminal law aspects of cyberwarfare, considering that cyberwarfare attacks performed during war or even at peacetime are considered criminal offences by all EU countries. Furthermore, the EU procedural mechanisms for prosecuting cyberwarfare crimes and the EU institutions responsible for cooperation in criminal matters are all presented.

2. Substantive law on cyberwarfare and cyberwarfare crimes

The goal of this chapter is to analyse the substantive legal content regarding cyberwarfare crimes, delving into both EU legislation and UN conventions. We present legal definitions of terms connected to cyberwarfare, such as cyberattacks, cyber espionage, and cyber spying. The main research question is whether these acts are defined as criminal acts in the EU and in the criminal legislation of EU Member States. Here, we must point out the diversity of criminal legislation in EU Member States and the question of whether some offences should be legalised at the EU level.

15 Khan, no date.

The EU has already compiled a list of so-called EU crimes in numerous legal acts; however, the question remains whether as to whether cyberwarfare crimes are included in these catalogues. The dilemma also remains regarding EU criminal law and whether there is a need for a new European Criminal Code that includes cyber offences and cyberwarfare crimes.

At the outset, it should be emphasised that cyberwarfare has neither a single nor a clearly established legal definition. In most cases where the topic is approached, there is reference to well-known forms of cyberattacks that most EU Member States have already defined as criminal acts. The specifics of cyberwarfare are that it is, first, connected with the army of an individual country (i.e. it is a military operation), and, second associated to a significantly wide range and scope of offence, as it attacks more important targets with significantly more repulsive motives – such as paralysing a country's national security via attacks on its infrastructure and technological centres. Therefore, for the purpose of this chapter, the term *cyberwarfare* will be used to describe cyber acts that compromise and disrupt critical infrastructure systems and which amount to armed attacks,[16] referring to attacks that intentionally cause destructive effects (i.e. death, physical injury to living beings, and/or the destruction of property). Only governments, state organs, and state-directed or state-sponsored individuals or groups can engage in cyberwarfare.[17]

The types of cyberwarfare attacks also vary according to the definition. For the purpose of this chapter, we categorise these attacks into the following: espionage (i.e. monitoring other countries to steal secrets), sabotage (i.e. harming state organisations or institutions), denial of service (also known as DoS) attacks to disrupt critical operations and systems, attacks that disable critical systems and infrastructure, propaganda attacks, economic disruption by targeting economic establishments, and surprise attacks in the context of hybrid warfare.[18] Importantly, no legal documents in the EU or UN directly address cyberwarfare, as the term has no clear legal definition. However, numerous legal documents can be used to address the topics of cyberwarfare and cyberwarfare attacks.

2.1. The UN Charter

Before a state engages in cyberwarfare, *jus ad bellum* (the right to use force) must be established, meaning that any kind of force must be legitimate and sanctioned by law. The rule of prohibition against the use of force is codified in Art 2 (4) of the United Nations Charter,[19] which states that a UN member state cannot threaten or use force against the territorial integrity or political independence of another state or in any way that diverges from the UN's purposes. Although Art.

16 Maras, 2016, pp. 10–20.
17 Ibid.
18 *Cyber Warfare*, no date.
19 *Charter of the United Nations and Statute of the International Court of Justice*, 1945.

2(4) does not use "armed" or a similar word, the question remains as to whether the article only prohibits military force and excludes non-military forms of coercion, such as economic sanctions or cyberattacks.[20] Given that the article is written in extremely general terms and that cyberwarfare attacks today represent a modern form of warfare, insisting on a position that completely rejects the possibility of cyberwarfare attacks being covered by Art. 2(4) is pointless. At the same time, it should be emphasised that force in the sense of Art. 2(4) in the context of cyberwarfare attacks can only be understood when the territorial integrity or political independence of a state is threatened by such attacks. Therefore, only serious military attacks that attack the very existence of the country are covered, and it is quite unlikely that the UN will condone only a cyberattack as a use of force according to Art. 2(4) of the UN Charter.

Meanwhile, according to Art. 51 of the UN Charter, countries can use self-defence as an exception to the prohibition against the use of force. This provision explicitly allows one state to use force in response to an armed attack by another state. It should be emphasised that cyberwarfare attacks can represent a form of self-defence against an attacker, and that such a defence must be necessary and proportional to the aggression. Another interesting feature of Article 51 is that it provides for the self-defence of a state only when the state is actually attacked by military forces – that is, when it is an armed attack, not when the state is attacked only by cyberwarfare attacks. However, denying the possibility of defending against cyberwarfare attacks would also be completely contrary to the UN ideology and the idea of a just war. There are thus two possible solutions, the first of which is we deny that cyberwarfare attacks are a form of modern armed warfare, do not regard them as a use of force in the sense of Art. 2(4), and it is not possible to use force to defend against such attacks according to Art. 51 of the UN Charter. Alternatively, and also a more modern solution, cyberwarfare attacks, when targeted at the territorial integrity or political independence of a state, can be considered a use of force according to Art. 2(4), and self-defence is possible against such a force according to Art. 51 of the UN Charter. According to the first solution, everything remains in a grey zone, and countries fight against these forms of attacks independently. According to the second solution, such attacks must be reported to the UN, where a solution is then sought within the framework of the UN Charter.

2.2. International Humanitarian Law: the Geneva conventions and Hague conventions

International humanitarian law is covered by the Hague[21] and Geneva Conventions,[22] which determine the fundamental rules of warfare and conduct prohibited in

20 *Use of force under international law*, 2024.
21 *The Hague Conventions*, 1890, 1907, 1954.
22 *The Geneva Conventions*, 1949.

every international armed conflict. The Hague Conventions deal primarily with the means and methods of warfare, the conduct of hostilities, and occupation, whereas the Geneva Conventions primarily govern the protection of war victims. The conventions, of course, do not mention cyberwarfare because it did not exist at the time these conventions were written. However, this does not mean that the general provisions of the conventions cannot apply to modern warfare. We believe that the conventions limit all forms of attacks towards civilians or civilian facilities, medical facilities, and other forms of war crimes if these attacks are conducted through classic military operations or cyberattacks.

A more complex question is whether cyber operations can trigger the application of international humanitarian law. International armed conflict 'exists whenever there is a resort to armed force between States'.[23] However, when is this point reached in situations involving cyber operations that do not physically destroy nor damage military or civilian infrastructure? This remains unclear. A potential solution would be the proposed hybrid model, which is derived from the established term for hybrid warfare,[24] and according to which cyberattacks can constitute a violation of Hague and Geneva laws when they are committed together with traditional war crimes, but not by themselves.

2.3. Rome Statute of the International Criminal Court

The International Criminal Court (also known as ICC or ICCt) is an intergovernmental organisation and international tribunal seated in The Hague, the Netherlands. It is the first and only permanent international court with jurisdiction to prosecute individuals for the most serious war crimes and crimes against humanity, as well as for crimes of genocide and aggression. It was established in 2002 with the multilateral Rome Statute,[25] which affords the legal basis for the functioning of the Court. The Court has its own problems, the main one being that most of the world's military superpowers (e.g. the USA, Israel, Russia, and China) have not signed the statute, so they do not recognise the jurisdiction of the International Criminal Court. However, almost all European countries are signatories.

The Rome Statute, in its Article 5, limits the jurisdiction of the Court to the most serious crimes against the international community. The Court has jurisdiction over the following crimes: (a) crimes of genocide, (b) crimes against humanity, (c) war crimes, (d) crimes of aggression.[26] Art. 6 of the Rome Statute defines the crime of genocide as acts committed with the intent of destroying a national, ethnic, racial, or religious group. Although killing a group with cyberattacks seems highly unlikely, deliberately inflicting on the group conditions of life calculated to bring about its

23 *Cyber Warfare: does International Humanitarian Law apply?*, 2021.
24 Weissmann et al., 2021.
25 *Rome Status of the International Criminal Court*, 1998.
26 *Rome Statute of the International Criminal Court*, 2002.

physical destruction, be it in whole or in part, is imaginable through attacks on basic life sustaining infrastructure (e.g. water and electricity). Cyberattacks can also be used in combination with traditional war crimes (i.e. hybrid model).

Crimes against humanity, after Art. 7 of the Rome Statute, refer to acts committed as part of a widespread or systematic attack directed at any civilian population. Most of the crimes against humanity are "physical" in nature (e.g. rape, murder, and enslavement); notwithstanding, if targeted at critical infrastructure for a population and thereby intentionally causing great suffering or injury to people, even cyberattacks could be a method of execution. It is important to note that such attacks must be part of a widespread or systematic attack on the population, and not just a singular attack against the national security of a country. Generally, cyberattacks are not defined as crimes against humanity. However, in combination with traditional war crimes (hybrid model), this would be possible.

Cyberattacks, when considering war crimes as defined in Art. 8 of the Rome Statute, are similar to crimes against humanity. Typically, cyberattacks on their own will not be defined as war crimes, but their combination with traditional war crimes (hybrid model) make their categorisation as such a possibility. War crimes must be committed as part of a plan or policy, or as part of a large-scale commission of, such crimes, and are grave breaches of the Geneva Conventions and of the laws and customs applicable in international armed conflict within the established framework of international law.[27]

The crime of aggression, as defined in Article 8 (bis) of the Rome Statute, refers to planning, preparation, initiation, or execution, by a person in a position where one can exercise effective control over or direct the political or military action of a state, of an act of aggression which, by its character, gravity, and scale, constitutes a manifest violation of the UN Charter. According to this definition, it is highly unlikely that a cyberattack by itself can be perceived as an act of aggression. This is because, first, it must be performed by a person in a specific position (military or state), and not by an ordinary individual or a hacker group. Second, because the act must be considered a violation of the UN Charter (para. 4 of Art. 2), where the standards are very high, in that the violation must be obvious in terms of its weight and scope. In light of these descriptions, it is very unlikely that the UN would regard cyberattacks as acts of aggression when they are conducted in isolation of other acts. However, it is possible that a cyberattack would accompany traditional war crimes, such as an unlawful war attack by one state on the integrity and sovereignty of another.

No provision of the Rome Statute specifically refers to cyberattacks or cyberwarfare, as this form of warfare was not yet present at the time the statute was drafted. However, it is entirely possible that cyberwarfare attacks will be covered in one of the already defined forms when the nature and scope of these attacks reach the level of intensity otherwise achieved by classic international crimes. A similar

27 Art. 8 of the Rome Statute, 1998.

point of view was shared by Khan, the prosecutor of the International Criminal Court, who described that:

> the tools used to commit serious international crimes constantly evolve – from bullets and bombs to social media, the internet, and perhaps now even artificial intelligence. As states and other actors increasingly resort to operations in cyberspace, this new and rapidly developing means of statecraft and warfare can be misused to carry out or facilitate war crimes, crimes against humanity, genocide, and even the aggression of one state against another.[28]

He further expresses that international criminal justice must adapt to this new landscape, as follows:

> While no provision of the Rome Statute is dedicated to cybercrime, such conduct may potentially fulfil the elements of many core international crimes, as already defined. In particular, the International Committee of the Red Cross has reiterated that cyber-attacks must comply with the cardinal principles of distinction and proportionality, and should only be directed against military objectives.[29]

The cyberspace is, therefore, not a special domain free from regulation, but rather a domain where international law has a clear role to play. Importantly, in modern warfare, the frontlines are no longer just physical, and digital frontlines can give rise to damage and suffering comparable to what the founders of the International Criminal Court sought to prevent.[30]

2.4. Convention on Cybercrime

Cybercrime is predominantly an international phenomenon, as new forms of criminal acts related to computer systems can spread worldwide very quickly. Accordingly, it is necessary to harmonise the international criminal legislation on cybercrime, especially owing to the processes involved in prosecuting cybercrime offences. Such prosecution requires not only clear definitions of related criminal acts in domestic criminal legislation, but also effective international cooperation between countries. Therefore, the purpose of the Convention on Cybercrime[31] is to unify measures at the criminal, material, and procedural levels and contribute to better prosecution of cybercrimes.

The Convention on Cybercrime contains a basic list of crimes that the signatories must accept, and at the time the Convention was adopted in 2001, this list was

28 Khan, no date.
29 Ibid.
30 Ibid.
31 *Convention of Cybercrime*, 2001; Council of Europe, 2001, CETS No. 185.

considered extremely advanced and elaborate, containing practically all the most important forms of criminal acts in information systems. However, the last 20 years since its adoption saw the rise of numerous new forms of cybercrime. This renders the Convention a representative of minimum standards that should be followed by practically every advanced criminal legislation in the world.

The Convention on Cybercrime was adopted by the Council of Europe on 23 November 2001, in Budapest, and had already been ratified in most European countries[32] and countries outside Europe, such as the United States of America, Canada, Japan, Israel, and Australia. The Convention is the main, fundamental document for harmonising the cybercrime-related regulations of EU countries and those of other countries that have ratified the Convention. The Convention also places strong emphasis on international cooperation in the prosecution of cybercrime. It is also necessary to emphasise the efforts of the Committee of Experts on Crime in Cyberspace, which is responsible for the effective implementation of the Convention's measures in the legislation of the signatory countries. The Committee's goal is to get as many countries as possible to sign and ratify the Convention.[33]

Prior to the adoption of the Convention, the basic document in this area was Recommendation No. R(95) 13 of the Council of Ministers of the Council of Europe[34] on criminal procedure problems related to information technology. After the creation of the Convention, the Council of Europe soon realised that it was necessary to add special racist and xenophobic crimes committed through information systems to the basic catalogue of crimes. For this purpose, the Council of Europe adopted the Additional Protocol to the Convention on Cybercrime, which deals with the criminalisation of racist and xenophobic acts committed in computer systems (CETS 189). The Protocol is an addendum to the Convention and is open to ratification by countries that have already ratified the Convention. The Additional Protocol was adopted and opened for ratification on 28 January 2003, but its adoption was slightly more restrained than that of the Convention, as only 42 countries signed the Protocol, while the Convention had 68 parties and 23 other signatories.

The title of the Additional Protocol already tells us how it deals with the various types of racist and xenophobic acts that can be carried out in computer systems or on the Internet. Unfortunately, some of the consequences of globalisation include the spread and dissemination of racism, discrimination, xenophobia, and other forms of intolerance, and the development of electronic communication and networks can contribute to racism and other xenophobic acts. In light of this, the Additional Protocol was adopted following two main purposes; the first is to harmonise criminal law in the field of combating racism and xenophobic acts committed on the Internet, and the second is to improve international cooperation in this area.[35] The legal in-

32 Ireland only signed the Convention, but did not accede to it.
33 *Explanatory report on the Convention on Cybercrime*, 2001, p. 4.
34 Council of Europe, R 95 13, 1995.
35 *Explanatory report on the Convention on Cybercrime*, 2001, p. 42.

terests protected by the Protocol are the equality of all people and equal protection of human rights against discrimination and racism. However, another legal interest stands in opposition to these rights, which is the freedom of expression, which led the Additional Protocol to be established as an attempt to strike a balance between the two interests and enable their protection.

In 2022, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) was put forward. While cybercrime proliferates in the context of increasingly complex ways of obtaining electronic evidence, mostly owing to these pieces of evidence being stored in foreign, multiple, shifting, and/or unknown jurisdictions, the powers of law enforcement remain limited by territorial boundaries. As a result, only a very small share of cybercrimes reported to criminal justice authorities leads to court decisions. In response, the Second Additional Protocol to the Convention on Cybercrime (CETS No. 185) provides a legal basis for the disclosure of domain name registration information, direct cooperation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate cooperation in emergencies, mutual assistance tools, and personal data protection safeguards.[36]

The Convention on Cybercrime comprises four chapters:

4. Use of terms
5. Measures to be taken at the national level (substantive criminal law and procedural law)
6. International co-operation
7. Final provisions

The most important part of the Convention for cyberattacks is on Chapter 2 on measures that must be taken at the national level. The substantive criminal law in it defines the criminal acts that must be outlined in the criminal codes of the signatory countries, whereas the procedural part defines the procedural provisions and guidelines that must be adopted in the procedural mechanisms of the signatory countries. The substantive criminal law part is represented by the following provisions in the Convention:

Art. 2 – Illegal access
Art. 3 – Illegal interception
Art. 4 – Data interference
Art. 5 – System interference
Art. 6 – Misuse of devices
Art. 7 – Computer-related forgery
Art. 8 – Computer-related fraud

36 *Details of Treaty No. 224*, no date.

Art. 9 – Offences related to child pornography
Art. 10 – Offences related to infringements of copyright and related rights

The Convention also defines international cooperation, in which provisions on a 24/7 network are at the forefront. This is an international information network that is supposed to be accessible 24 hours a day and seven days a week, through which signatory countries are supposed to exchange information and data related to cybercrime.

Regarding cyberwarfare attacks, the most relevant articles in the Convention are as follows: the notion of illegal interception under Art. 3, which can be used in cases of cyber-spying and espionage; the description on data interference under Art. 4; the description on system interference under Art. 5. These articles tackle issues that are present in any kind of cyberattack targeting an information system in the context of cyberwarfare, be it a denial of service attack, attacks to disrupt critical operations and systems, attacking and disabling critical systems and infrastructure, economic disruption by targeting economic establishments, surprise attacks in the context of hybrid warfare, or even sabotage. The difference between the offences in Arts. 4 and 5 is that data interference comprises damage, deletion, deterioration, alteration, or suppression of only computer data, whereas system interference disrupts the functioning of an information system as a whole, even if it is performed by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.

Computer-related forgery (Art. 7) and fraud (Art. 8) are connected to cyber-spying and espionage. Moreover, Art. 6 on the misuse of devices could be associated to all types of cyberwarfare attacks because it criminalises any kind of production, sale, procurement for use, import, distribution or otherwise making available of devices, programs, or codes that enable the perpetrator to perform one of the criminal offences listed in the Convention. This means that all those who aid in cyberwarfare attacks by providing software or hardware to attackers will be criminally liable together with the perpetrators.

It should be emphasised that the Convention on Cybercrime, with its Additional Protocols, is not the only regulation governing the field of cybercrime worldwide. Since it was written more than two decades ago, it has become relatively outdated in some respects. During this period, the EU has taken over legislative initiatives in Europe, with the largest shift in the field of European legislation being associated with the Treaty of Lisbon (i.e. the Treaty on European Union and the Treaty on the Functioning of the European Union, TFEU) in 2009. This Treaty gave the EU a legal basis for the adoption of criminal law directives to ensure the effective implementation of EU policies. Before the adoption of the Treaty of Lisbon, the EU intervened in criminal law mainly through framework decisions and conventions.[37] Interven-

37 *The 1995 Convention on the Protection of the EU's Financial Interests and its Protocols, Council Regulation (EC, Euratom) no. 2988/95 of 18 December 1995 on the protection of the financial interests of the European Communities in relation to administrative sanctions.*

tions by the EU were mainly focused in the area of the EU's financial interests, but they also spread to other criminal areas (e.g. child pornography).[38] According to the Treaty of Lisbon, instead of just being a provider of framework decisions and conventions, the EU can now adopt normal community instruments (regulations, directives, and decisions) with direct effect on the territory of EU Member States.[39]

2.5. Directive EU 2013/40/EU on attacks against information systems

Directive EU 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA continues the unifying work of the Convention on Cybercrime. The main objective of the Directive is to approximate the criminal law of Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and relevant sanctions. It is also aimed at improving cooperation between competent authorities, including the police and other specialised law enforcement services of EU Member States, competent specialised EU agencies and bodies (e.g. European Union Agency for Criminal Justice Cooperation [Eurojust], European Union Agency for Law Enforcement [Europol], and its European Cyber Crime Centre, and the European Network and Information Security Agency, ENISA).[40]

The Directive sets out substantive measures and contains articles on improved cooperation at the procedural level. Some of the material measures are on the following topics: illegal access to information systems (Art. 3); illegal system interference (Art. 4); illegal data interference (Art. 5); illegal interception (Art. 6); tools used for committing offences (Art. 7); incitement, aiding, abetting, and attempt (Art. 8). The definitions are quite similar to those of the Convention on Cybercrime; therefore, states that have signed the Convention are already familiar with these offences. A novelty that the new Directive brings is the demanded penalties from EU Member States, which now vary from at least two years of imprisonment for less serious offences to at least five years for more serious offences. The Directive also adds the criminal liability of and sanctions for legal persons that must be implemented in the national law of EU Member states. Still on a procedural perspective, the Directive also defines the jurisdiction for the prosecution of cyberattacks (Art. 12) and demands the exchange of information relating to the offences described in the

38 *Council Framework Decision 2004/68/PNZ of 22 December 2003 on combating the sexual exploitation of children and child pornography.*

39 This applies especially to the so-called "European crimes", which include terrorism, human trafficking, sexual exploitation of women and children, illicit traffic of illegal drugs and weapons, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime. The Council can only establish additional "European crimes" unanimously and with the consent of the European Parliament.

40 Preamble of the Directive, 2013, p. 1.

Directive (Art. 13). The EU Member states must also monitor and prepare statistics on cybercrime (Art. 14).

With regard to cyberwarfare attacks, the Directive does not bring about drastic changes. Attacks that could already be prosecuted based on the definitions in the Convention on Cybercrime can also be prosecuted based on this Directive. The central definition of a cyberwarfare attack is the illegal interference in systems and data (Arts. 4 and 5 of the Directive, respectively). It is important to note that this is a mandatory Directive with which all EU Member States must comply, and even the United Kingdom and Ireland have notified their wish to take part in the adoption and application of this Directive. Although the Directive does not include as broad a spectrum of cyber offences as the Convention does, it still mostly covers all offences related to cyberwarfare attacks by sanctioning illegal interception, data interference, and system interference, and aiding and abetting these offences.

2.6. Directive EU 2022/2555 on measures for a high common level of cybersecurity

The Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), is aimed at building the cybersecurity capabilities of the EU. It also focuses on mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing incidents, thus contributing to the EU's security and to the effective functioning of its economy and society.[41] The EU emphasises that during the war in Ukraine, cyberattacks went hand in hand with conventional military tactics, and their main purposes were destroying and disrupting the functioning of government agencies and organisations that managed critical infrastructure, as well as undermining confidence in the country's leadership. Basic services, such as transport, healthcare, and finance, are increasingly dependent on digital technologies and are therefore extremely susceptible to cyberattacks.[42] This is the main reason why the new Directive was adopted at the EU level, namely, so as to ensure the greatest possible information and cyber security in the EU.

In December 2020, the European Commission and the European External Action Service (also known as EEAS) presented a new EU cybersecurity strategy, aimed at making the EU more resilient to cyber threats and securing that all citizens and businesses can enjoy the full benefits of trusted and reliable services and digital tools. Part of the new EU cybersecurity strategy was adopted by the EU Cybersecurity Act, which focused on strengthening the ENISA and establishing a cybersecurity certification framework for products and services. Meanwhile, the ENISA plays a key role

41 Preamble to the Directive, 2022, p. 1.

42 *Cybersecurity: why reducing the cost of cyberattacks matters*, 2021.

in setting up and maintaining the EU's cybersecurity certification framework by preparing the technical grounds for specific certification schemes.[43]

Part of this new EU cybersecurity strategy also involves the new NIS 2 Directive.[44] This Directive lays down measures aimed at achieving a high level of cybersecurity across the EU and improving the functioning of the internal market. It defines that EU Member States must adopt national cybersecurity strategies and designate/establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity, and computer security incident response teams (also known as CSIRTs). Specifically, Chapter III of the NIS 2 Directive is dedicated to cooperation at the EU and international levels. The Directive also establishes a Cooperation Group composed of representatives of EU Member States, the Commission, and ENISA (Art. 14). Furthermore, it describes a network of national computer security incident response teams to promote swift and effective operational cooperation among EU Member States (Art. 15), and the European Cyber Crisis Liaison Organization Network (also known as EU-CyCLONe), which should support the coordinated management of large-scale cybersecurity incidents at the operational level and ensure the regular exchange of relevant information among EU Member States and EU institutions, bodies, offices, and agencies (Art. 16). Chapter IV of the Directive deals with cybersecurity risk-management measures and reporting obligations, while Chapter II deals with coordinated cybersecurity frameworks, including national cybersecurity strategy (Art. 7), competent authorities and single points of contact (Art. 8), national cyber crisis management frameworks (Art. 9), and computer security incident response teams (Art. 10).

Although the new NIS 2 Directive does not include new definitions of criminal offences and, therefore, does not directly address definitions of cyberwarfare crimes, the goal of the Directive is to prepare a defence strategy against such attacks for the information systems of EU Member States. The new Directive also imposes stricter requirements (vs. prior similar documents) and obligations for EU Member States regarding cybersecurity, especially in terms of supervision. Moreover, the Directive improves the enforcement of these obligations through the harmonisation of sanctions across all EU Member States. In fact, the major purpose of the Directive is to improve cooperation between EU Member States, especially in the event of major cyber incidents. Therefore, while the Directive in question does not define criminal acts under which individual forms of behaviour in the context of cybercrime could be placed, nor specifically refers to cyberwarfare, it does generally apply to all cyberattacks and cybercrimes.

43 *The EU Cybersecurity Act*, no date.

44 *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).*

2.7. Criminal Law of the European Union

One question that can arise here, based on the expositions in the prior sections, is the following: is there a European criminal law? That is, in the sense that the EU acts as a sovereign state, formulates criminal acts, carries out criminal prosecution, and sanctions the perpetrators of criminal acts? The answer is a resounding no. However, we can speak of European criminal law when the EU protects its financial interests through legislation enforced on its Member States, but only in this sense. Regardless of this situation, the EU still depends on its Member States to enforce the regulations, as the EU itself has no means physically coerce individuals. As Ambos writes,

> the designation European criminal law is a kind of umbrella term covering all those norms and practices of criminal and criminal procedural law based on the law and activities of the EU and the Council of Europe and leading to widespread harmonisation of national criminal law.[45]

Therefore, there is no comprehensive, self-contained European criminal law or justice system, but more of an umbrella-like system that connects different entities, organs, and legislations in the EU towards the investigation and prosecution of transnational crimes.[46] This is especially for those crimes connected to the financial interests of the EU.

There are debates on whether the EU should have its own criminal code, which would in turn represent the next level of harmonisation and unification of criminal offences in the EU. However, an initial problem with such a venture is the sovereignty of Member States. The criminal code of a country presents the ultimate expression of its legal authority, in that each state declares conduct that is unacceptable to such a degree that it will use its physical coercion capabilities to enforce its rules. By renouncing its own criminal code and leaving it in the hands of another authority, the sovereignty of the state becomes questionable; in such a scenario, someone who does not follow the elected legitimate rule of the state becomes able to enforce criminally prohibited conduct, or conduct that would otherwise be seen as prohibited. It seems that EU Member States are not (yet) ready to take such a step, and is questionable if they ever will. Unlike other federations, the EU was primarily established as an economically-unifying union of completely different sovereign states, which in turn have different languages, established nationalities, long histories, and different origins. Another problem regarding the potential of the EU having a criminal code would be the different interpretations of the law in different jurisdictions; this problem could be solved by establishing a common European High Court, whose precedents should be binding on inferior courts throughout Europe.[47] A final problem, at least for the

45 Ambos, 2018, p. 14.
46 Ambos, 2018, p. 15.
47 Cadoppi, 1996, pp. 2–17.

purposes of this study, is that the TFEU does not include an authorisation for the EU to create codes of law. A criminal code should include more than a compilation of European Directives and Framework Decisions. Still, in the TFEU, its Art. 83/1 gives the EU the option to adopt directives that establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crimes with a cross-border dimension and that are of such nature or impact that there is a special need to combat them at the EU level.[48]

Therefore, no independent supranational European criminal law has been created beyond the EU's competence. However, the national criminal law of EU Member States is influenced by EU law through its Directives, Framework decisions, and other normative guidelines, as well as by the principle of mutual recognition. This Europeanised criminal law is complemented by the creation of different European institutions in the area of criminal law, which in turn have their own goals and authorisations.[49]

As defined in Art. 83/1 of the TFEU, the European Parliament and Council may adopt directives to combat cross-border crimes that threaten the (economic) interests of the EU. The areas in which criminal unification is possible are also defined in this article, and are the following: terrorism, human trafficking, sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime. The EU, therefore, has some power to harmonise the criminal law of its Member States. This harmonisation takes place through an assimilation obligation on the part of EU Member States, and the harmonisation of substantive criminal law by means of the EU's competence to approximate and annex criminal law pursuant to Art. 83(1) and (2) TFEU. Indeed, making use of these competences, the EU has issued several directives[50] aimed at harmonising national criminal law.[51] The list of crimes described in Art. 83/1 of the TFEU was included in the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) and the jurisdiction of Europol and Eurojust in Art. 4.1 of the Council Decision establishing the European Police Office (Europol) (2009/371/JHA) and its Annex, and later in Annex D of the Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters.

The 32 offences related to this article can be grouped into crimes defined in EU law, typical crimes in national laws, and crimes within the jurisdiction of the International Criminal Court. The list of offences ranges from crimes such as terrorism to swindling and arson, and there is no guiding system or principle on how the list was

48 Long, 2011, pp. 49–52.

49 Ambos, 2018, p. 15.

50 For example, *Directive (EU) of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.*

51 Šepec and Schalk-Unger, 2023, pp. 203–224.

made. More specifically, it includes cross-border crimes (e.g. terrorism and drug trafficking), crimes that relate specifically to the EU (e.g. protection of its financial interests), and ordinary offences such as fraud, arson, and extortion. Some offences are formulated in a vague, broad manner (e.g. corruption, organised or armed robbery), while others only capture a criminal phenomenon (racism and xenophobia), raising doubts as to whether such phenomena can be referred to as offences.[52]

This list also includes computer-related crimes, which in turn feature probably one of the vaguest definitions on the entire list. Computers and information systems have become essential tools for the functioning of modern society and are commonly used when committing criminal offences. Accordingly, a unified and comprehensive list of crimes performed against or with the help of computer systems has been compiled under the Convention on Cybercrime, which lists the following offences: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to infringement of copyright and related rights. However, only computer-related forgery and fraud are defined under the chapter Computer-related offences (others are defined under the chapters named Offences against the confidentiality, integrity and availability of computer data and systems; Content-related offences; and Offences related to infringements of copyright and related rights). The offence list of the Convention was later expanded with the Additional Protocol, which criminalises acts of a racist and xenophobic nature committed through computer systems. Therefore, it is quite evident that the term "computer-related crimes" could include a vast list of different offences, the problem being here that such wideness of the term opposes the principle of legality, as it is not clear which offences are really meant with the term. This dilemma was at least partly solved by the Directive 2013/40/EU,[53] which includes five different offences: illegal access to information systems, illegal system interference, illegal data interference, illegal interception, and tools used for committing offences. This entails that only these offences should be covered by the category "computer-related crime" in the Annex D of the EIO Directive. That is, cyberwarfare attacks, which are included illegal system interference, illegal data interference, and illegal interception, are covered in the lists of EU crimes after Art. 83/1 of the TFEU. Cyberwarfare attacks are therefore treated by the EU as crimes with a cross-border dimension of such nature and impact that they need special treatment, and require the harmonising of legislation at the EU level to prosecute such crimes more efficiently. The proof of this is the adopted Directive 2013/40/EU on attacks against information systems.

Therefore, for the purpose of prosecuting cyberwarfare attacks within the EU, there is no need to amend EU legislation or adopt new EU Directives on the criminal material level, as the adopted legislation already covers the main offences. However,

52 Ambos, 2018, p. 435.

53 *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing council framework decision (2005/222/JHA).*

current EU legislation is written mainly for the purpose of normal cyberattacks (by hacker groups or individuals), and does not contemplate cyberwarfare attacks or operations against EU Member States. If the EU develops a system of joint military defence, legislation that provides further protection to the EU against cyberwarfare attacks could be a viable option in the future.

3. EU procedural measures of cooperation in criminal matters for prosecuting cyberwarfare crimes

The judicial cooperation in the EU is based on the principle of mutual recognition. In accordance with Art. 82 of the TFEU, this includes rules and procedures for ensuring recognition throughout the EU of all forms of judgments and judicial decisions, preventing and settling conflicts of jurisdiction between EU Member States, training of the judiciary and judicial staff, and cooperation between judicial or equivalent authorities of EU Member States in relation to proceedings in criminal matters and the enforcement of decisions. This means that the EU has a legal basis for implementing procedural measures that can be used to prosecute cyberwarfare crimes internationally. When prosecuting cross-border crimes, EU Member States are not alone nor isolated from each other, but rather can and should rely on joint mechanisms of cooperation at the EU level to facilitate criminal prosecution. This means that EU Member States can help each other in the cross-border prosecution of cyberwarfare crimes not only politically but also legally; what this means is that the EU Member State does not decide on cooperation politically, but rather is legally bound to such cooperation by EU legislation.

With the Treaty of Lisbon, police and judicial cooperation was transferred to the area of justice and home affairs. Consequently, mutual legal assistance in the EU has developed from classic treaty-based assistance to a system of executive assistance based on mutual recognition. The European Parliament and the Council can jointly establish minimum rules for the approximation of law in ordinary legislative procedures.[54]

Indeed, the approximation of procedural law is possible according to Art. 82 of the TFEU. Minimum rules can be established through directives in the fields of the admissibility of evidence, rights of individuals, and rights of crime victims. Furthermore, legal assistance in the EU includes areas of extradition and other mutual assistance in criminal matters (e.g. questioning witnesses, gathering evidence, searching, and confiscating) and enforcement (e.g. the execution of foreign judgments and decisions).[55]

54 Ambos, 2018, pp. 411–412.
55 Ibid., pp. 414–415.

On this premise, the EU has adopted numerous conventions, directives, and framework decisions to facilitate mutual cooperation and recognition among its Member States. This means that the Member State is never alone in gathering evidence or prosecuting a criminal offence when the offence was committed internationally or in the territory of other EU Member States. For the purposes of prosecuting cyberwarfare crimes, the most relevant procedural measure of the EU may be the European Investigation Order.

3.1. European Investigation Order

Directive 2014/41/EU on the European Investigation Order in criminal matters (EIO-Directive) established a single comprehensive framework, based on the principle of mutual recognition, that allows EU Member States to obtain evidence from other Member States. This Directive replaced existing frameworks for the gathering of evidence, namely the 2000 EU Mutual Legal Assistance Convention, Framework Decision 2008/978/JHA on the European evidence warrant, and Framework Decision 2003/577/JHA on the freezing of evidence. The EIO-Directive was adopted in April 2014, giving EU Member States (except Ireland and Denmark) three years for its transposition. After its implementation, the EIO-Directive soon became the leading legal instrument for gathering evidence in the EU, revolutionising EU cooperation in criminal matters. By providing deadlines for execution and introducing a practical form in Annex A that was soon adopted in practice, the EIO did not remain a theoretical concept but a commonly used and useful tool for legal practitioners dealing with offences that have a cross-border element in the EU.

The EIO-Directive also introduced rules relating to the types of procedures in which it can be used, conditions for its usage, rules of recognition and execution, and legal safeguards for refusal of execution, thereby safeguarding the basic rights of the defendants and preventing serious infringements to the criminal procedures of EU Member States (e.g. demanding an execution of an investigative measure that is not legally implemented in the executing state). The overall objective of introducing a standard EIO form, available in all official languages of member States, was to simplify formalities, improve quality, and reduce translation costs. Despite the fact that the form itself could be improved, research shows that practitioners consider the EIO form usable in their current formulations, and regularly use it.[56] In this form, the issuing authority describes the criminal offence being investigated, the applicable criminal law, and the types of measures requested. If there are no grounds for refusing the EIO, the executing authority of the EU Member State shall execute the demanded EIO. However, the executing authority shall have some margin to check the proportionality of the EIO when the latter is not in conformity with the

56 Šepec, Dugar and Stajnko, 2023, p. 123.

constitutional standards of the executing state. There is also the possibility of replacing the requested measure with a similar one providing the same results.[57]

Of course, it would be utopian to expect such a commonly used legal instrument to be completely absent of any theoretical or practical shortcoming. In light of this reality, an international project called EIO-LAPD was funded by the European Commission, which aimed to identify these difficulties and find solutions. The thorough analysis of the legal framework and practical dilemmas conducted by the project highlighted possible solutions for various shortcomings of the EIO form, including the following: dilemmas on accepted languages in urgent cases; transmission of EIOs and electronic evidence via insecure communication channels; video conference tool use; requests for non-existent measures; the *ne bis in idem* non-recognition ground; coercive measures; speciality rule; requests for issuing EIOs by the defence.[58] Despite its shortcomings, the EIO remains the main cooperative measure at the EU level for gathering and exchanging evidence in criminal prosecutions and trials, including those pertaining to cyber warfare attacks.

In the near future, we can expect facilitations in the development of the e-Evidence Digital Exchange System (also known as eEDES), and a push for its implementation in all EU Member States, as digital evidence is ever more prevalent in criminal law and new problems regarding securing such data are constantly emerging. We expect this to be the next stage of the EU development on the topic of evidence exchange in criminal matters. However, this push to regulate the exchange of digital evidence should not come at the cost of amending other pressing issues in the EIO-Directive, such as rethinking the existing legal framework from the perspective of the rights of the accused and the *ne bis in idem* principle.[59]

EU Institutions for cooperation in criminal matters

This section presents the main EU Institutions that cooperate in criminal matters. We are interested in understanding the roles of these institutions, whether they are of a political nature, and whether they have legal authority. One question that can be proposed here would be the following: what are the capabilities and jurisdictions of EU institutions regarding cyber and cyberwarfare crimes? Can EU Member States refuse the authority of EU institutions, or do they have to submit and cooperate with them? What is the legal basis of EU institutions, what are their main goals, and how effective are they in prosecuting international crimes?

To respond to these questions, the following subsections explore the main EU institutions connected to criminal offences.

57 Bachmaier-Winter, 2023, p. 295.
58 Ibid., pp. 127–137.
59 Šepec, Dugar and Stajnko, 2023, p. 136.

Europol

The Europol is the most important agency for police cooperation in the EU, having the main goal of supporting and strengthening EU Member States' law enforcement agencies, especially the police. Importantly, the Europol does not have executive power and cannot arrest people or conduct investigations independently. This is evident from Art. 88 of the Treaty on the Functioning of the European Union, which states that the application of coercive measures should be the exclusive responsibility of competent national authorities.

The Europol was established in 1998 in the context of the Third pillar of the Europol Convention.[60] In 2009, the Council of Europe repealed the primary Convention and adopted the Europol Council Decision, which was later repealed by Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol). The Europol is based on The Hague, in the Netherlands, and serves as the central hub for coordinating criminal intelligence and supporting the EU's Member States in their efforts to combat various forms of serious and organised crime, as well as terrorism.

The Europol facilitates the exchange of information and intelligence, provides analytical support, and offers specialised training and expertise. Some of the key areas of focus of the Europol, as listed in the Annex I to the Europol Regulation, include drug trafficking, human trafficking, cybercrime, money laundering, and counterterrorism. This list is quite similar to that of crimes for which the Council Framework Decision 2002/584/JHA on the European Arrest Warrant and other EU instruments of mutual recognition do not require a double criminality standard.[61] This poses questions about the exact authorities of the Europol, as these offences are defined vaguely and without a system behind the seemingly random list of offences; this contradicts the principle of legality as the core criminal law principle of national legal systems. The principle of legality in relation to the categories of offences listed in Annex I to the Europol Regulation can be fully respected only when a clear legal definition of each listed offence can be found in EU legislation. If there is no clear normative content provided by the EU, then the differences between the legal definitions of certain offences can vary across EU Member States to such an extent that there is no clear legal definition of the offence at all.[62]

As Europol is competent to support and strengthen national authorities in preventing and combating computer-related crimes (Art. 3 and Annex I to the Europol Regulation (EU) 2016/794), the principle of legality can once more be questioned, as "computer crimes" is a very vague definition that includes numerous offences, and it is not clear which offences are really meant with the title "computer-related offences".

60 *Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office* (Europol Convention). See also Ligeti and Giuffrida, 2023, p. 362.
61 Ligeti and Giuffrida, 2023, p. 367.
62 Šepec and Schalk-Unger, 2023, p. 207.

This dilemma was at least partly solved by the Directive 2013/40/EU,[63] which includes five different offences, as follows: illegal access to information systems, illegal system interference, illegal data interference, illegal interception, and tools used for committing offences. Therefore, only these offences should be covered by the category "computer-related crime" in Annex I to the Europol Regulation.

Regarding computer crimes, which cover cyberwarfare attacks, Europol has important data processing tasks that include gathering and processing information, incorporating criminal intelligence, and performing strategic and operational analyses. Although the Europol does not have coercive powers, the institution's information gathering generates knowledge that can lead to evidence useful in national court procedures.[64] The Europol is, therefore, an essential partner of national authorities when discovering cybercrime offences with international elements. This becomes especially evident when Europol coordinates the organisation and execution of investigations together with Member States, or within the framework of joint investigative teams.

For this purpose, Art. 4(l) of the Europol Regulation (EU) 2016/794 stipulates that the body shall develop Union centres of specialised expertise to combat certain types of crime falling within the scope of Europol's objectives, particularly the European Cybercrime Centre. To prevent and combat cybercrime, which are associated with network and information security incidents, Europol lays down measures to ensure a high level of network and information security across the EI, and cooperates and exchanges information with national authorities competent on the security of network and information systems. Member States should also supply Europol with information about any alleged cyberattacks affecting EU bodies located in their territory.[65] Furthermore, when coordinated action among several EU Member States is necessary, the Europol may recommend the establishment of Joint Investigative Teams (also known as JITs), and Europol can participate in and support these teams through the collection and analysis of intelligence data.[66] As Europol is an agency of the EU, judicial control of its concrete measures is exercised by the Court of Justice of the European Union **(**CJEU).

Eurojust

The Eurojust was established in 2002 and is located in The Hague, in the Netherlands. The main goal of the agency is to improve cooperation among EU Member States on the investigation and prosecution of serious cross-border and organised crime. Eurojust started functioning as a provisional unit (Pro-Eurojust),[67] and was

63 *Directive 2013/40/EU of the European Parliament and of the Council of 12 august 2013 on attacks against information systems and replacing council framework decision* (2005/222/JHA).
64 Ligeti and Giuffrida, 2023, p. 385.
65 Preamble of the Europol Regulation (EU) 2016/794, paras. 13 and 30.
66 Ambos, 2018, p. 565.
67 *Council Decision 2000/799/JHA*.

later established by Council Decision 2002/187/JHA. Its legal basis was amended thrice, specifically by Council Decisions 2003/659/JHA and 2009/426/JHA, which broadened its original powers,[68] and finally by Regulation (EU) 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust). The latter is the current legal basis for Eurojust's authority, and was adopted because of the need for enhanced cooperation among EU Member States for establishing the European Public Prosecutor's Office (EPPO).

Eurojust was established to address the need for centrally coordinated cross-border prosecution of the most serious crimes committed in the EU. This can only be achieved using a decentralised network of national contact points, which in turn made necessary to the creation of an additional central body in which representatives of the judicial authorities of all Member States are located.[69]

Furthermore, the Eurojust was conceptualised as an independent, collegial judicial institution of the EU that should have its own legal personality. Eurojust's main tasks are the initiation of criminal investigations and prosecutions, the coordination of investigations and prosecutions in EU Member States, and the strengthening of the judicial cooperation of EU Member States.[70] Still, Eurojust lacks any real formal investigative power, as the decision to investigate or prosecute a crime in a EU Member State falls under national authorities. The right of initiative shows only the Lisbon Contracting Parties' willingness to grant Eurojust this right.[71]

The Eurojust's jurisdiction covers crimes listed in Annex 1 of the Regulation (EU) 2018/1727, which encompasses the familiar list of EU crimes, including "computer-related crimes". Therefore, according to the principle of legality, Eurojust has jurisdiction over the computer-related crimes listed in the Directive 2013/40/EU, which includes the five different offences mentioned before in this paper. Although the list is slightly more detailed than the first one proposed in the European Arrest Warrant framework decision (e.g. the new list specifies fraud affecting the financial interests of the European Communities, while the first list only included fraud and swindling), there has been no change in computer crimes. This means that Eurojust has competencies over cybercrime and cyberwarfare offences when committed against or in EU Member States. An exception here is Denmark, which owes to the special regime foreseen in Protocol no. 22 of the Lisbon Treaty.

It should be emphasised that when the EPPO starts its investigative and prosecutorial functions, Eurojust should not exercise any competencies. The exception to this rule, meaning that Eurojust would maintain its competence, is when a request is made by the authorities of EU Member States, or a request is issued by the EPPO itself. The same can be said for crimes on which EPPO has no competence, or on

68 Hernandez Lopez and Jimenez-Villarejo Fernandez, 2023, p. 387.
69 Ambos, 2018, p. 569.
70 Ibid., p. 570.
71 Ibid.

which it has decided not to exercise such competence.[72] Still, even as the EPPO takes over the investigation, Eurojust still keeps the obligation to mutually consult and cooperate with the EPPO. Furthermore, Eurojust can assist EU Member States even in crimes not listed in Annex 1 of the Regulation (EU) 2018/1727, meaning that it could offer assistance even in computer-related crimes not defined in Directive 2013/40/EU. Finally, Eurojust can support EU Member States in investigating or prosecuting a crime that only affects that Member State (i.e. without an international element) if the case could have an impact at the EU level.[73]

Today, Eurojust, together with the EPPO, represents the peak of investigative and judicial cooperation in the EU. Eurojust was designed to allow EU Member States to perform their investigative tasks more effectively while preserving their national and operational independence.

The CJEU

The CJEU was established in 1952 and represents the judicial branch of the EU. It comprises two separate courts, the Court of Justice and the General Court; however, it also includes specialised courts. The CJEU is thus a supranational institution, meaning that it is empowered to exercise powers and functions otherwise reserved to states.

Accordingly, the CJEU is the EU's chief judicial authority and oversees the uniform application and interpretation of EU law. The CJEU interprets the EU law to ensure that it is applied in the same manner to all EU Member States. The Court also settles legal disputes between national governments and EU institutions, and can sometimes be used, under specific circumstances, by individuals, companies, or organisations to act against an EU institution if the party states that the institution somehow infringed upon their rights.[74] Through the communisation of the former third pillar, the CJEU's jurisdiction has been extended to the area of police and judicial cooperation, and is now part of "justice and home affairs".[75]

The CJEU performs the following functions. Interpreting the law: the national courts of EU countries are required to ensure that EU law is properly applied; however, courts may interpret EU law differently. If a national court doubts the interpretation or validity of EU law, it can ask the Court for clarification. The same mechanism can be used to determine whether a national law or practice is compatible with EU law. The Treaty of Lisbon further strengthened the role of the CJEU as the sole interpreter and enforcer of EU law.[76] Enforcing the law: when a national government fails to comply with EU law, a procedure can be initiated by the European Commission or by

72 Hernandez Lopez and Jimenez-Villarejo Fernandez, 2023, pp. 390–391.
73 Ibid.
74 *Court of Justice of the European Union (CJEU)*, no date.
75 Ambos, 2018, p. 573.
76 Ambos, 2018, p. 573.

another EU country to request the CJEU to enforce EU law. Annulling EU legal acts: when an EU act is believed to violate EU treaties or fundamental rights, the CJEU can be asked to annul it. In fact, private people can ask the Court to annul an EU act that directly affects them, including criminal law and procedures. This ensures that the EU takes actions when the Parliament, Council and Commission must make certain decisions, and choose to do not. In such cases, a complaint can be issued to the CJEU. Sanctioning EU institutions: any person or company who has had their interests harmed as a result of the action or inaction of the EU or its staff can initiate this procedure in the CJEU.[77]

In the past, the CJEU has generally adopted a pro-EU, integrationist stance, and advocated the principle of mutual recognition, assuming mutual trust, although there is no solid basis for this in national law and practice. This has led the Court to be often characterised as a driving force of EU integration.[78] Although the CJEU has no direct function regarding cyberwarfare offences, it will play an important role in interpreting EU legislation and enforcing it on EU Member States. For example, the actual use of Directive EU 2013/40/EU on attacks against information systems, and/or of directives that provide cybersecurity protection (e.g. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union), depends on the interpretation of this legislation by the CJEU. However, it is worth noting that the CJEU is not in charge of conducting criminal trials against defendants of cyberwarfare offences, and this task instead falls to the national courts of EU Member States. Regardless, in the case of a misunderstanding pertaining to the legal regulations of the EU, the CJEU could get involved to interpret EU law. This, of course, does not mean that the CJEU will pass a judgment, as this task always falls under the national court of EU Member States.

The EPPO

The EPPO is the EU's first independent prosecuting office. It has the power to investigate, prosecute, and bring to judgment crimes against the EU budget, such as fraud, corruption, and serious cross-border value added tax fraud.[79] The EPPO was established out of the need for an independent, decentralised prosecutorial body to combat crimes affecting the financial interests of the EU. More specifically, it was introduced with Regulation 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (RegEPPO), and started to function on 1 June 2021. It was approved after two decades of political and doctrinal debate, specifically thanks to the enhanced cooperation mechanism of the Treaty of Lisbon under Art. 86 of the TFEU. Still, the investigative and prosecutorial powers

77 *Court of Justice of the European Union (CJEU)*, no date.
78 Ambos, 2018, p. 573.
79 *European Public Prosecutor's Office*, no date.

of the EPPO throughout the territory of EU Member States are limited to crimes affecting EU financial interests, as defined by Directive 2017/1371.[80]

The EPPO is based on the separation of prosecutorial and adjudicatory powers. The first is in the hands of the EPPO, while the latter is in the hands of national authorities. This was a political compromise, since EU Member States were not willing to submit to a full-fledged EU criminal justice system, which in turn implied the need for a EU criminal justice system.[81] As things stand now, EU Member States still control the judging process and overall judicial control over criminal proceedings; therefore, the judicial process is still in the hands of national authorities.

The EPPO is accountable only to the European Parliament, Council, and Commission. It comprises its Central Office at The Hague, in the Netherlands, and European Delegated Prosecutors coming from and located in EU Member States. The Central Office consists of the College, Permanent Chambers, European Chief Prosecutors, Deputy European Chief Prosecutors, European Prosecutors (each Member State has one), and the Administrative Director. There exists a hierarchy between delegated prosecutors at the central level and at the Member State level, which may often lead to tension and conflict, as delegated prosecutors at the national level must follow the instructions of the European prosecutor.[82]

At a given point in time, there was a raging debate as to what would be the material and territorial competence of the EPPO. Regulation 2017/1939 defined in Art. 22 that the EPPO shall be competent in respect of the criminal offences affecting the financial interests of the EU that are provided for in Directive (EU) 2017/1371, as implemented by national law, irrespective of whether the same criminal conduct could be classified as another type of offence under national law. This implies that the principle of dual criminality does not apply. The EPPO shall also be competent for offences regarding participation in a criminal organisation, as defined in Framework Decision 2008/841/JHA, if the focus of the criminal activity of such a criminal organisation is to commit any of the offences referred to in Directive (EU) 2017/1371. Furthermore, the EPPO shall also be competent for any other criminal offence inextricably linked to criminal conduct affecting the financial interests of the EU that are provided for in Directive (EU) 2017/1371. The material competence of the EPPO is, therefore, quite broad and could include cyberwarfare attacks; however, it would include so only when the attack is inextricably linked to criminal conduct affecting the financial interests of the EU, as the Directive (EU) 2017/1371 does not directly include computer crimes or cyberwarfare crimes. Therefore, the EPPO will not be the main protagonist when prosecuting cyberwarfare crimes on the EU territory. This task will instead fall to the national prosecutors of the EU Member State that was the target of the cyberwarfare attack. As aforementioned, the exception here would be

80 Allegrezza, 2023, p. 413.
81 Ibid., p. 414.
82 Ambos, 2018, p. 575.

attacks inextricably linked to criminal conduct affecting the financial interests of the EU, where the EPPO would maintain its material competence.

Additionally, Art. 23 of Regulation 2017/1939 defines the territorial competence of the EPPO, describing that it is competent if the offences were committed in whole or in part within the territory of one or several EU Member States, or committed by a national of a EU Member State. Importantly, the EPPO regulation follows the model of shared competence, where the EPPO only intervenes if the national authority is unable or not in a position to sufficiently protect the EU's financial interests itself. Thus, the decision whether to initiate an investigation right away or not falls to the EPPO. It remains, notwithstanding, that disagreements lend the final decision to fall to the EU Member State.[83] This means that the EPPO cannot overrule the decision of a Member State if the latter decides that it can protect the EU's financial interests.

If the EPPO decides to prosecute a crime under its jurisdiction, prosecution at the national level is executed by the European delegated prosecutor under the procedural law of the EU Member State where the trial will be held. This of course leads to abnormalities, as while the substantive law under which the EPPO functions is at least partly harmonised in Directive (EU) 2017/1371, the procedural law always varies depending on the EU Member State where the trial takes place.

Office de Lutte anti-fraude

The Office de Lutte anti-fraude (OLAF) was established on 28 April 1999, by Commission Decision 1999/352/EC and Regulations 1073/99 (EC) and 1074/99 (Euratom), as an independent investigative Commission agency. The OLAF's legislation was amended numerous times, the latter being Regulation NO 883/2013 (OLAF Regulation) and Regulation No. 2020/2223.[84] The main goal of the OLAF is to detect fraud against the EU budget, acts of corruption, and serious misconduct against EU institutions. It conducts independent investigations into fraud and corruption involving EU funds, as well as other serious illegal activities against the financial interests of the EU.[85] Furthermore, the OLAF investigates corruption in EU institutions and proposes anti-fraud legislation and EU policies.

It performs both external and internal investigations. External investigations are performed at the EU Member State level, where the OLAF depends on the competent national investigative authority and is not permitted to adopt any coercive measures.[86] Internal investigations refer to irregularities within the EU's institutions, offices, and agencies, whereby the OLAF has a much broader authority, can carry out investigations, examine and confiscate documents and data media, and gather

83 Ibid., p. 576.
84 Cahn, 2023, p. 330.
85 Ibid., p. 331.
86 Ambos, 2018, p. 561.

information from EU officials.[87] Nonetheless, the OLAF is obliged to surrender its investigation to national authorities in the case of criminal proceedings, as it cannot prosecute suspects by itself.

Although the OLAF is an important EU institution regarding financial frauds against the interests of the EU, when the topic is cyberwarfare attacks or even ordinary cyber offences, it does not play an important part, having practically no competencies or authority for investigating such offences. Furthermore, the OLAF is not a law enforcement agency; therefore, even if it had any jurisdiction over cyberwarfare or cyber offences, it would not be the institution coordinating the gathering of evidence and criminal prosecution of such offences. Some even question the nature of the OLAF and the task of its staff; are they investigators, prosecutors, or something in between?[88]

5. Conclusion

Cyberwarfare has neither a single definition nor a clearly established legal definition, but at its core, it means using computer technologies to disrupt or destroy an adversary's information systems and networks. In most cases, these are already known forms of cyberattacks, and which most EU Member States have already defined as criminal acts. The specifics of cyberwarfare are thus that it is connected with the army of an individual country, which configures a military operation, and that the range and scope of related offences are significantly wider, as cyberwarfare involves attacks to more important targets with significantly more repulsive motives, such as paralysing a country's national security via damages to its infrastructure, and technological centres.

No legal documents in the EU or UN directly address cyberwarfare, as the term has not yet a clear legal definition. However, we can use numerous legal documents that indirectly address the topic of cyberwarfare and related attacks, such as the UN Charter, International humanitarian law, the Rome Statute of the International Criminal Court, Convention on Cybercrime, Directive 2013/40/EU, and Directive EU 2022/2555.

There is no European criminal law, such that the EU does not act as a sovereign state, formulate criminal acts, carry out criminal prosecution, nor can sanction perpetrators of criminal acts. Instead, the EU can only protect its financial interests through the legislation enforced by its Member States, hence depending on EU Member States to enforce its regulations; that is, in itself, the EU has no means of physical coercion.

87 Ibid., p. 562.
88 Xanthaki, 2016.

To prosecute cyberwarfare attacks within the EU, there is no essential need to amend EU legislation or adopt new EU Directives on the criminal material level, as the adopted legislation already covers the main offences. However, current EU legislation is written mainly for the purposes of normal cyberattacks (e.g. by hacker groups or individuals), and not specific for the purpose of war attacks or war operations against EU member states. If the EU develops a system of joint military defence in the future, legislation that provides further protection to the EU against cyberwarfare attacks could turn out valuable.

At the procedural level, the EU has a legal basis (Treaty on the Functioning of the European Union) for implementing procedural measures that can be used to prosecute cyberwarfare crimes at the international level. When prosecuting such cross-border crimes, EU Member States are not alone or isolated from each other, but rather can rely on joint mechanisms of cooperation (the most important being the European Investigation Order) at the EU level, which can be used to facilitate criminal prosecution. This means that EU Member States can help each other in the cross-border prosecution of cyberwarfare crimes. This cooperation is not political but of a legal nature, meaning that the EU Member State does not decide on cooperation politically, but is legally bound by EU legislation to cooperate. For this purpose, the EU can use its institutions for cooperation in criminal matters, including the Europol, Eurojust, OLAF, CJEU, and EPPO.

References

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2003) Council of Europe, CETS No. 189, Strasbourg, 28 January 2003.

Allegrezza, S. (2023) 'The European Public Prosecutor's Office (EPPO)' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law.* Cambridge: Cambridge University Press, pp. 413–438.

Ambos, K. (2018*) European Criminal Law.* Cambridge: Cambridge University press; https://doi.org/10.1017/9781316348628.

Bachmaier-Winter, L. (2023) 'Further Mutual Legal Assistance' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law.* Cambridge: Cambridge University Press, pp. 283–305; https://doi.org/10.1017/9781108891875.017.

Barrett, N. (1997) *Digital crime, Policing the Cybernation*. London: Kogan Page.

Cadoppi, A. (1996) 'Towards a European Criminal Code', *European Journal of Crime, Criminal Law and Criminal Justice,* 4(1), pp. 2–17; https://doi.org/10.1163/157181796X00104.

Cahn, O. (2023) 'EU Anti-Fraud Policy – Administrative Investigations – EPPO' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law.* Cambridge: Cambridge University Press, pp. 229–360.

Charter of the United Nations and Statue of the International Court of Justice (1945) United Nations.

Clough, J. (2010) *Principles of cybercrime*. Cambridge: Cambridge University press; https://doi.org/10.1017/CBO9780511845123.

Consolidated version of the Treaty on the Functioning of the European Union (2012) OJ C 326, 26 October 2012.

Consolidated version of the Treaty on the Functioning of the European Union PROTOCOLS – Protocol (No 22) on the position of Denmark (2012) OJ C 326, 26 October 2012.

Convention of Cybercrime (2001) Council of Europe, CETS No. 185, Budapest, 23 November 2001.

Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) (1995) OJ C 316, 27 November 1995.

Convention on the Protection of the EU's Financial Interests and its Protocols, Council Regulation (EC, Euratom) no. 2988/95 of 18 December 1995 on the protection of the financial interests of the European Communities in relation to administrative sanctions (1995) OJ L 312, 23 December 1995.

Council of Europe (2001) 'Explanatory report on the Convention on Cybercrime' Budapest, 23 November 2001.

Council Framework Decision 2004/68/PNZ of 22 December 2003 on combating the sexual exploitation of children and child pornography (2004) OJ L 013, 20 January 2004.

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002) 2002/584/JHA, OJ L 190, 18 July 2002.

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (2009) OJ L 121, 15 May 2009.

Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002) OJ L 063, 6 March 2002.

Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (2003) OJ L 245, 29 September 2003.

Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (2009) OJ L 138, 4 June 2009.

Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (2017) OJ L 283, 31 October 2017.

Digmelashvili, T. (2023) 'The Impact of Cyberwarfare on the National Security', *Future Human Image*, 2023/19, pp. 12–19; https://doi.org/10.29202/fhi/19/2.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013) OJ L 218, 14 August 2013.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (2014) OJ L 130, 1 May 2014.

Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (2017) OJ L 198, 28 July 2017.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022) OJ L 333, 27 December 2022.

Directive (EU) of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (2018) OJ L 156, 19 June 2018.

The Geneva Conventions (1949) Geneva, 12 August 1949.

Gibson, W. (1984) *Neuromancer*. London: Voyager.

The Hague Convention (II) on the Laws and Customs of War on Land (1899).

The Hague Convention III – XII (1907).

The Hague Convention for the Protection of Cultural Property (1954).

Hernandez Lopez, A., Jimenez-Villarejo Fernandez, F. (2023) 'Eurojust' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law*. Cambridge: Cambridge University Press, pp. 361–386; https://doi.org/10.1017/9781108891875.022.

Khan, K.A.A. (no date) 'Technology Will Not Exceed Our Humanity', *Digital Front Lines*. [Online]. Available at: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/ (Accessed: 15 August 2023).

Ligeti, K., Giuffrida, F. (2023) 'Europol' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law*. Cambridge: Cambridge University Press, pp. 361–386; https://doi.org/10.1017/9781108891875.021.

Long, N. (2011) 'Towards a European Criminal Law Code?', *EIPAScope*, 2011/1, pp. 49–52.

Maras, M.H. (2016) *Cybercriminology*. Oxford: Oxford University Press.

McCarthy, J. (1990) 'Generality in artificial intelligence' in Lifschitz, V. (ed.) *Formalizing Common Sense*. Norwood: Ablex Publishing Corporation, pp. 226–236.

Recommendation no. R(95) 13 of the Council of Ministers of the Council of Europe (1995) Council of Europe R (95) 13, 11 September 1995.

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (2018) OJ L 295, 21 November 2018.

Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations (2000) OJ L 437, 28 December 2020.

Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-fraud Office (OLAF) and repealing Regulation (EURATOM) No 1074/1999 (2011) European Commission, Brussels, 17 March 2011.

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (2016) OJ L 135, 24 May 2016.

Rome Status of the International Criminal Court (1998) UN Security Council.

Šepec, M., Schalk-Unger, L. (2023) 'Special part of EU criminal law: the level of harmonization of the categories of offences listed in annex D in EU legislation and across selected member states' in Ambos, K., Heinze, A., Rackow, P., Šepec, M. (eds.) *The European investigation order: legal analysis and practical dilemmas of international cooperation*. Berlin: Duncker & Humblot, pp. 203–224.

Šepec, M., Dugar, T., Stajnko, J. (2023) 'European Investigation Order – A Comparative Analysis of Practical and Legal Dilemmas' in Ambos, K., Heinze, A., Rackow, P., Šepec, M. (eds.) *The European investigation order: legal analysis and practical dilemmas of international cooperation.* Berlin: Duncker & Humblot, pp. 123–137.

Wimann, G. (2005) 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict and Terrorism,* 28(2), pp. 129–149; https://doi.org/10.1080/10576100590905110.

Wall, D.S. (2005) 'The Internet as a Conduit for Criminal Activity' in Pattavina, A. (ed.) *Information Technology and the Criminal Justice System*. Lowell: Sage Publications, pp. 77–98; https://doi.org/10.4135/9781452225708.

Weissmann, M., Nilsson, M., Palmertz, B., Thunholm, P. (eds.) (2021) *Hybrid Warfare, Security and Asymmetric Conflict in International Relations*. London: I.B. TAURIS; https://doi.org/10.5040/9781788317795.

Xanthaki, H. (2016) 'The Kessler case should lead to a reform of OLAF', *Euractiv*, 20 June 2016. [Online]. Available at: https://www.euractiv.com/section/justice-home-affairs/opinion/the-kessler-case-should-lead-to-a-reform-of-olaf/ (Accessed: 10 November 2023).

Court of Justice of the European Union (CJEU) (no date). [Online]. Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en (Accessed: 20 October 2023).

Cyber-Attack Against Ukrainian Critical Infrastructure (2021) *America's Cyber Defense Agency*, 20 July 2021. [Online]. Available at: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (Accessed: 30 August 2023).

Cybersecurity: why reducing the cost of cyberattacks matters (2021) *European Parliament*, 12 October 2021. [Online]. Available at: https://www.europarl.europa.eu/news/en/headlines/society/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters (Accessed: 10 October 2023).

Cyber Warfare: does International Humanitarian Law apply? (2021) *ICRC, International Committee of the Red Cross*, 25 February 2021. [Online]. Available at: https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law (Accessed: 30 August 2023).

Cyber Warfare (no date) *Imperva*. [Online]. Available at: https://www.imperva.com/learn/application-security/cyber-warfare/ (Accessed: 25 August 2023).

Details of Treaty No.224 (no date) *Council of Europe*. [Online]. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (Accessed: 25 September 2023).

The EU Cybersecurity Act (no date) *European Commission*. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (Accessed: 10 October 2023).

European Public Prosecutor's Office (no date) *European Anti-Fraud Office*. [Online]. Available at: https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/european-public-prosecutors-office_en (Accessed: 20 December 2023).

Struxnet (no date) *ScienceDirect*. [Online]. Available at: https://www.sciencedirect.com/topics/computer-science/stuxnet (Accessed: 30 August 2023).

Use of force under international law (2024) *Justia*, June 2024. [Online]. Available at: https://www.justia.com/international-law/use-of-force-under-international-law/ (Accessed: 25 August 2023).

IV.6

NEW TYPES OF WARFARE: INFORMATION AND HYBRID WARFARE

Chapter 16

Information Warfare Tactics and Techniques

Stjepan Groš

Abstract

Information warfare, disinformation, fake news, and similar terms are frequently used in public discourse. It is clear from real-world examples that these concepts represent a substantial danger for democratic countries, polarise societies as regards public health, and generally prevent rational and informed discussion. Yet, combating disinformation proves very difficult. Something must be done, but the question is what. The premise of this chapter is that we cannot counter disinformation if we do not agree on what we are fighting against; that is, we cannot do something if we do not know what the adversaries are using against us. In cybersecurity, databases of tactics and techniques of adversaries' behaviour have proved very useful for defence. Knowing about different types of attackers, their motives, and capabilities has also proved beneficial. Therefore, we are set to replicate this success in the case of information warfare and information operations. To achieve these goals, we review the terminology and define information warfare in a narrow sense and then discuss information operations, their relation to military domains and information space, and the domains in which information operations are run. In doing so, we determine that information operations are intertwined with and appear in all military domains. The core part of this chapter lists the tactics and techniques adversaries use for information operations. We then review the logistics support adversaries might use for information operations; moreover, we define threat sources and threat actors and classify them based on their motivations and capabilities. Finally, we map the operations run during Operation Denver to the tactics and techniques presented in this chapter to illustrate their use.

Stjepan Groš (2024) 'Information Warfare Tactics and Techniques'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 701–754. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_16

Keywords: warfare, information warfare, information operations, cyber warfare, tactics, technics, procedures, mitre att&ck, operation Denver

1. Introduction

In today's hyperconnected world, information flows faster than ever, reaches more people than ever, and allows everyone to express their opinion that can be heard by a large audience. This state of affairs has brought many advantages and improvements, such as an easier and more enjoyable life, better and faster scientific achievements, faster industrial development, and more innovative products and services. These are just some examples of the many positive changes this new age has brought to humanity.

Significant advances are also being made in the field of machine learning (ML), specifically large language models (LLMs). ChatGPT was made publicly available on 30 November 2022, and it showed impressive performance while being available to everyone with an internet connection. This caught the eye of the mainstream media and the general public. This undoubtfully revolutionised ChatGPT's application in different aspects of everyday work and caused a huge societal shift towards this new technology.

Yet, all these advancements have a dark side that threatens the society in new – yet unexplored – ways. Some of the issues we face are new. For example, due to the rapid flow of information, we have less time to process it in an appropriate way, and thus we are more susceptible to low-quality information. However, many of the issues have been present in the society in one form or other for decades. What is new in this case is that the advancement of technology allows more people to be targeted, faster than ever, with more information than ever – and not just with information but also unverified rumours, uninformed opinions, and plain malicious information. This creates social problems that might impact even national security. In addition, what was once only a capability of nation states and their secret services is now in the reach of less resourceful groups, even individuals, which further exacerbates the already dire situation.

An example of how this situation can escalate is the manipulation witnessed during the 2016 United States (US) presidential election, which arguably changed the course of the election. Other examples include false information spread about COVID-19, because of which more people died than would have without such false information. Thus, problems created by such technological development threaten human lives and the core of today's society – its democratic processes. However, this is only the tip of the iceberg.

In October 2021, a workshop was organised to assess how new technology in the form of LLMs will impact the society and individuals through so-called influence

operations.[1] The workshop gathered 30 experts from the fields of artificial intelligence (AI), influence operations, and policy analysis. The workshop concluded that there are significant changes ahead of us; however, some uncertainties were present at that time, which prevented the workshop from drawing more specific conclusions.

In essence, we are caught between fast technology development on the one hand and the slow changes in individuals and even slower changes in the society on the other. Added to this are the limited information processing capabilities of individuals, not to mention that processing is prone to errors due to human nature. It is inevitable that individuals and the society will have to change, but even if we know what changes we need to make, their implementation will take time. To conclude, as the saying goes, we live in interesting times, and we need to understand this development and the tools and techniques that will allow us to counter the negative effects of development. At the same time, we must not prevent the benefits to be utilized and developed further.

This chapter tries to tackle the negative effects of technological development by structuring the field in a way that makes thinking and analysing the current and future states of affairs easier as well as more organised, effective, and efficient. Emphasis is placed on information flow and, more specifically, on information warfare, which we think is concerned with information flow – as we see later in this chapter. However, be aware that this is only a part of the whole story. There are many other aspects to be considered, such as the psychological and cognitive aspects (warfare) as well as propaganda, which are not dealt with in this chapter. As already mentioned, we are tackling a very complex problem, and this chapter takes just a small step in finding its solution.

To organise the field, this chapter focusses on developments in cybersecurity that turned out to be useful and were consequently used frequently – specifically, the "cyber kill chain"[2] and "MITRE ATT&CK pattern".[3] Cyber kill chain is a model of the adversary's behaviour while attacking a target. The idea is that if we know how the attacker behaves, we can recognise him sooner and stop him by disrupting his processes during an attack. This idea of the cyber kill chain is taken from military sciences where the kill chain has been used for some time. The other significant development in cybersecurity that influenced this work is the MITRE ATT&CK pattern. The MITRE ATT&CK pattern aims to be a public knowledge database that contains information about all known attackers and their tactics, techniques, and sub-techniques. The difference between the cyber kill chain (or modelling of the attacker's behaviour) and the MITRE ATT&CK pattern is that the latter is not a model but a union of all models. Many tools are being produced to detect and contain attackers that heavily rely on the MITRE ATT&CK pattern.

1 Goldstein, 2023.
2 Hutchins et al., 2011.
3 Strom et al., 2020; MITRE ATT&CK, no date.

One goal of this chapter is to try to create a database similar to the MITRE ATT&CK pattern for disinformation campaigns. Having such a database can open up new possibilities for studying and understanding adversaries' behaviour. Namely, it would be possible to compare adversaries and predict their behaviour, which in turn might help with countering them. Moreover, it could be possible to foresee behaviour that was not yet utilised but could be in the future.

Finally, one additional important inspiration comes from information security, a branch of security used in companies that deals with the protection of companies' information resources. One interesting fact about information security is that it does not deal with the content of what it is protecting. The content falls within the realm of business and, as such, is taken for granted by information security practitioners. Another interesting fact about information security is that it deals with information in any form and not only digital information that is stored in some computer or transmitted via a network. These facts inspired us to treat information operations as not being strictly related to information and communication technologies (even though this is their most frequent form today). More importantly, this allowed us to better distinguish between information warfare and other forms of warfare.

This chapter has additional goals. The main goal is to introduce tactics and techniques that can be used by adversaries when spreading disinformation. Because techniques depend on technical elements of the environment in which everything happens, we also review the important technical elements of this environment.

This chapter is structured as follows. First, Section 2 Background reviews the basic terminology used throughout the chapter. Then, Section 3 Information Operations discusses the central topic of this chapter as well as some connected terms in more detail. In this section, we introduce the information lifecycle, which forms the basis for a set of tactical steps. This chapter's main contribution is discussed in Section 4 Tactics and Techniques, which lists the tactics and some techniques for each tactic. In several cases, we delve into more detail in the form of sub-techniques. Certain support services for spreading disinformation are created potentially independently and are used on an as-needed basis. Some of these services are described in Section 5 Logistics Support. Moreover, we analyse the threat actors and threat sources in Section 6 Threat Sources and Actors, as it is very important to identify the adversary targeting us. Finally, in Section 7 Example of the Application of Tactics and Techniques, we present a concrete example where we map one information operation to the tactics and techniques we described. The chapter ends with conclusions and future work in Section 8 Conclusions.

2. Background

As stated in the introduction, we are concerned primarily with information warfare. Therefore, in this chapter, we tackle the term "information warfare" as well as other related terms such as "information operations". Since a lot is happening in this and other related fields, a lot of materials are published on this topic on almost a daily basis; consequently, there is a lot of misuse of different terms for various reasons. Here, we are trying to organise and relate different terms in a way that will allow us to proceed into more detail without being distracted by the interrelation between or confusion regarding the different terminology used (or abused) in the literature.

2.1. Warfare and Information Warfare

We start with the definition of the term "warfare", and accordingly, we define the term "information warfare". The term "warfare" is a more technical rather than legal term, and it refers to the activity of fighting a war, including the "weapons and methods" that are used. In other words, warfare encompasses "tactics and techniques" available for use in a war. The exact set of weapons and methods used determines specific types and subtypes of warfare, such as cyberwarfare, space warfare, ground warfare, naval warfare, aerial warfare, information warfare, and hybrid warfare.

It is important to note that even though the term "warfare" is associated with war and it is implicitly assumed that it is used in war by a military, "warfare" can also be used by other groups and individuals. The key to understand this is that the tactics and techniques of traditional warfare require a lot of resources and are thus mainly accessible to militaries. On the other hand, cyberwarfare and information warfare, which make extensive use of information and communications technology, are available to a much wider audience with significantly lower resources.

Additionally, anyone can try to use the tactics and techniques of classical warfare, but because of the characteristics and restrictions of the physical world, as well as restricted resources, the effect is weak and restricted to a small area. On the contrary, few individuals can achieve a much bigger effect by using information warfare compared to that using classical weapons, mainly because of the information space and its characteristics, as well as information technology. That is, thanks to the Internet, everyone can reach everyone else throughout the world. Furthermore, by using readily available services, a much wider audience can be reached with a limited set of resources, such as by writing a blog or publishing videos on YouTube.

This reachability and availability have an important implication – potentially many more actors can engage in these activities, all of whom have varying degrees of resources and motives. This point must be considered because it is a significant departure from the things as they used to be.

In conclusion, in this chapter, "warfare" refers to tactics and techniques used to achieve the required end state. Depending on the set of tactics and techniques, we talk about different forms of warfare. One goal of this chapter is to define tactics and techniques that compose information warfare. More specifically, information warfare involves tactics and techniques used to deliver information (disinformation) to specific targets.

2.2. Related Forms of Warfare

Besides information warfare, some other closely related but not identical forms of warfare include psychological warfare, cognitive warfare, and propaganda warfare. There could be other forms as well, because it is fashionable to call something "warfare," as it raises the level of seriousness. An example is "disinformation warfare" whose validity is debatable, but many other such terms appear in the literature and especially on the Internet. Yet, the three terms psychological, cognitive, and propaganda warfare are important; the terms psychological and propaganda warfare have been known for almost a century and used much longer than that. All these types of warfare, along with information warfare, target the cognitive and psychological processes of human beings, and that is why we consider them in depth.

Human beings can be targeted in different ways in the context of information and related warfare, all ending in a human being thinking or feeling something. To make a distinction, feelings fall within the realm of psychology, while thinking is a cognitive process. The thinking and feeling of human beings can be influenced by information delivered to and received by them, which is then interpreted. Alternatively, individuals can be influenced by direct physical contact, which is also a form of information delivery.

It is not so easy to discern the two influences – that is, information received and physical contact – but here are three examples to better illustrate the difference. First, persons being targeted are given leaflets with text describing how superior their opponent is. Second, persons being targeted see enemy planes flying and demonstrating their superior performance. Finally, persons being targeted learn about the building of an artificial island, which is by itself difficult to maintain and is of questionable (classical) military value.[4]

The first example is clearly based on information received by the targeted persons. The second example is a combination of physical activity (airplanes manoeuvring) and information received (planes through sight). We classify such activity as direct physical contact since the information itself was directly perceived by the targeted persons, without employing any means of conveying information, such as the Internet, newspaper, and radio. The third example is based on information received, because few people have the ability to go and see the island for themselves;

4 Southerland, 2016.

that is, the majority will read somewhere about such an island. Thus, we classify this example as information received.

Based on these examples, we can define the two influences, information received and physical contact, as follows: Influence by information received is any indirect means of impacting people, where people did not directly see or feel the event that occurred but somehow received information about the event. Physical contact (or experience) allows a person to directly see or feel something and accordingly create an opinion or enter a psychological state.

An additional important factor is that humans have basic instincts and higher-level thought processes. These two concepts are interrelated but can be influenced separately. Moreover, because of a disconnection between the two, one can be harmed without the other being harmed. For example, a demonstration of force might induce a feeling of fear in a person, even though a rational approach (if used) can lead to the conclusion that this demonstration is actually irrelevant. Cases with such a disconnect between basic instincts and higher-level thought processes are interesting and important; however, they can be addressed by future research, as they are outside the scope of this chapter. Rather, we focus on the levels of the human mind, feelings, and cognitive processes. Accordingly, we compare different warfare types and their connection to information warfare.

Psychological and cognitive warfare differ in the same way that psychology and cognitive psychology do. Psychology, in the broad sense, studies the mind and behaviour, but there are different schools of thought. Since psychological warfare as a field of study originated in the 1940s,[5] it originally used methods and approaches from behavioural psychology. As psychology progressed as a scientific discipline, so did psychological warfare. Cognitive psychology is a school of thought within psychology that emerged in the 1960s. We can conclude that while psychological warfare in the narrow sense and cognitive warfare differ in terms of methods and approaches, both try to influence the human mind and behaviour. Moreover, psychological warfare in the broad sense encompasses any means to influence the mind and behaviour; thus, it involves both psychological warfare in the narrow sense and cognitive warfare.

In this chapter, we treat information warfare as tactics and techniques to convey information to humans; however, information warfare itself does not deal with "what" is necessary to convey to humans to achieve a desired psychological state. This falls within the realm of psychological and cognitive warfare. In other words, we are not interested in the psychological and cognitive aspects of spreading false information. Note that, in the context of psychological and cognitive warfare, physical experience can be used to achieve the desired ends, which is obviously not in the realm of information warfare.

One important type of warfare used today is "hybrid warfare", which is thoroughly analysed in the next chapter from the legal perspective. There is no agreed

5 Farago, 1941.

upon definition of what exactly is hybrid warfare. Considering the definition of warfare in this chapter, we treat hybrid warfare as a set of tactics and techniques that are taken from other types of warfare – psychological, information, cognitive, cyber, and propaganda – and from more traditional ones, such as asymmetric, chemical, electronic, and drone warfare. The question of which tactics and techniques might be assumed under hybrid warfare should be answered empirically by analysing the hybrid operations (if we could agree on what hybrid operations are) and taking observed tactics and techniques into the set of tactics and techniques that define hybrid warfare. This endeavour is obviously very broad and uncertain. Therefore, this chapter does not analyse hybrid warfare but instead information warfare. This is because information warfare is a narrower area of activity and thus more manageable; at the same time, principles used for information warfare can also be used for the analysis of hybrid warfare.

Finally, we also mention "propaganda",[6] a term closely related to information warfare. Propaganda, unlike information warfare, has a fixed target – the general public – and the goal of influencing public opinion and making it favourable to whoever is utilising the propaganda. To achieve its end-state, propaganda combines various aspects of psychological, cognitive, and information warfare. For that reason, we see propaganda only as a special case of these three warfare types.

2.3. War

The concept of war is very important and interesting to consider. It is defined as follows:[7]

> War – in terms of international law – is a legal condition, a state of armed conflict between different states or nations within a state. Whether a state is at war – legally speaking – depends upon the status of opponents, e.g., whether they are states, nations, peoples, belligerents, or insurgents. Not every act of hostility or use of armed force necessarily creates a war in terms of international law, but if it does, it produces legal consequences for the parties and for the entire international community. The legal consequences are determined primarily in the UN Charter.

This definition is very useful in the case of conflicts between states when both sides' armies are engaged. However, the definition does not tell much about what differentiates war from non-war states; it only shows that certain legal conditions exist in the case of war that do not exist in non-war states. Additionally, much of international law is dedicated to the rules for how war is fought to prevent unnecessary loss of human lives or unnecessary destruction.

6 Smith, 2024.
7 Dinstein, 2011.

Yet, the second part of the 20th century showed that in the modern world, asymmetric and other forms of conflicts are much more frequent, in which one side is so dominant that the other side avoids direct conflict. This complicates the state of affairs because it is not war in the classical sense.

Cyberwar is especially interesting in this context. There is a lot of debate about whether cyberwar is possible[8] and what could be achieved by it. Armies around the world declared cyberspace the fifth domain of war and started establishing separate branches just to fight the cyberwar. Nevertheless, the Russian aggression in Ukraine in 2022 brought a lot of surprises in terms of warfare in general and cyberwarfare and information warfare in particular. It turned out that the only way of achieving decisive gains was classical warfare and not cyberwarfare. This does not mean that no cyberwarfare occurs but that classical military actions are more influential at this point.

This development has impacted the use of information warfare and all activities in the information space. Namely, the results of information warfare activities can be expected in the medium to long term. Thus, if someone is preparing for war, activities in the information space must start much sooner and prepare the ground for activities during the war. Russia itself imposed strict control of its information space along with the repressive measures it has applied for a long time. This resulted in the absence of almost any opposition to its war efforts – at least publicly. This is interesting for at least two reasons. First, it creates an asymmetric situation in which information flows freely on one side of the conflict, while there is no free flow of information on the other side. The consequences for the spread of disinformation is obvious. Disinformation spreads easily on the side with the free flow of information, and Russia has used this intensively.

As regards the definition of war, it used to mean that nation states were on opposing ends. Today, for various reasons, this is not the case anymore. Apart from the asymmetric conflicts mentioned above, development of technology empowered additional groups to engage with the nation state or with a part of it, making it a national security problem. This has additional consequences as well. Therefore, resources invested in conflict are not a good measure to assess whether it is a war or not. In modern warfare, because of technological developments, it is possible to achieve significant damage with only a small amount of resources invested by the adversary.

2.4. Information Operations

War is an activity occurring on operational and tactical levels that has the goal of achieving or supporting the strategic end-state. The operational level of war connects the strategic end-state with its tactical-level activities; that is, it organises tactical-level activities to achieve the strategic goals. Because one operation might not be enough to achieve the strategic end-state, multiple operations could be run, all

8 Rid, 2012; Stone, 2013.

of which strive to achieve the same strategic end-state and are collectively called "campaigns".

In the context of information warfare, we are interested in "information operations" and, consequently, "information campaigns". Information operations are activities that organise the tactics and techniques of information warfare to achieve the strategic goals. In this chapter, we use the terms "information operations" and "information warfare" interchangeably; although these terms are not the same formally, it should be clear which term we are referencing from the context.

It is interesting to look at an alternative definition of an information operation, provided by Facebook in its report on abuse of the platform:[9]

> … actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion (we refer to these as 'false amplifiers').

This definition is interesting for three reasons. First, it acknowledges that one side of the conflict can be a non-state actor, that is, it could be anyone. It also opens up the possibility that both sides are non-nation states. For example, outside actors try to compromise certain political movements within the country. This will impact the nation state as a whole but nevertheless is not a conflict between the outside actor and the nation state itself. Even though this is an interesting case, we are not interested in such cases in this book. Instead, this book is meant to help policymakers in decision-making regarding information operations. Therefore, we assume that the side suffering from information operations is a nation state or some part of it. Second, this definition explicitly mentions false news and fake accounts, in addition to disinformation traditionally tied with information warfare. This makes the definition appropriate in the context of Facebook but is too restrictive for our case, as we look at a much broader picture. The third reason this definition is interesting is that it enumerates the specific goal of information operations – manipulation of public opinion. We believe this is also too restrictive as the goal of information operations might be to target specific parts of the society, not necessarily those who form or influence public opinion. To conclude, the definition of information operations given by Facebook is a restricted version of our definition.

An additional term used frequently in the literature is "influence operations". We will use the definition given by Rand Corporation for this term:[10]

9 Weedon, Nuland and Stamos, 2017, p. 5.
10 Larson et al., 2009, p. 2.

> Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives.

This definition is much broader as it allows the use of not just information warfare but also other means such as diplomatic and even military action. At the same time, it specifically names the US as the actor running influence operations as well as a beneficiary of those operations. Obviously, influence operations, as defined by RAND, overlap with information warfare and information operations, but they are distinct concepts.

Information operations, when executed, are controlled by the "information operation operator". The task of an information operation operator is to coordinate activities, allocate resources, assign tasks, etc. We use the expressions "operator" and "adversary" interchangeably in this chapter, as they have the same meaning.

It is important to be aware that information operations are not something new. They have been conducted for a long time, although the information space used to be significantly different than it is today. An interesting example of an information operation from before the advent of the Internet and information technology is Operation Denver.[11] This operation was conducted by the Soviet Union to convince people in the West that the acquired immunodeficiency syndrome (AIDS) was developed in secret laboratories. This example is significant as it also shows how running such an operation before the Internet was a complicated, long-running process requiring a lot of resources, and thus it was not accessible to many. Such an operation also depended more on luck as many related developments were not under the control of the information operation operator.

2.5. Disinformation

What is interesting in the case of information warfare is the question of what is a weapon. We argue in this chapter that the so-called bullets in such warfare comprise misinformation, disinformation, and malinformation, while the weapons are all the technical means of generating, publishing, and distributing misinformation.

According to the Council of Europe,[12] the terms misinformation, disinformation, and malinformation have the following meanings. "Misinformation" occurs when false information is shared, but no harm is meant, such as a satire taken seriously, typos, and errors. "Disinformation" occurs when false information is knowingly shared to cause harm, such as when fabricated or deliberately manipulated content is designed and shared to mislead. Finally, "malinformation" occurs when genuine information is shared to cause harm, often by moving what was designed to stay

11 *Operation INFEKTION*, 2024.
12 Wardle and Derakhshan, 2017.

private into the public sphere, such as deliberate publication or leaking of private information and deliberate changes to the context of genuine content.

Unfortunately, while distinctive, these definitions are hard to apply in practice. First, the case of when disinformation is created and then shared by someone who believes in it is not covered by any of these terms. This case involves unintentional sharing of false information, which is classified as misinformation, but it started as disinformation. The key point is that using these definitions involves determining someone's motive and, more importantly, someone's state of mind, which is extremely difficult. Malinformation, on the other hand, is easy to classify, but the problem is that it might include disinformation as well; this was the case in 2016, when the Democratic National Committee's email leaks also contained disinformation. In that case, it is difficult to say if it is malinformation or disinformation. For this reason, we will use the term disinformation for any false information shared that causes harm to individuals, groups, or the society at large.

As seen in the case of Facebook, the concept of fake news[13] is also used frequently lately.[14] While fake news might be misinformation, it more commonly appears in the form of online disinformation with an added twist of imitating journalistic form to seem more credible. This leads us to the conclusion that fake news, and disinformation in general, have two components: (1) content and (2) form. Content depends on the purpose of disinformation and the target, while form is more a technical issue. We will get back to this distinction when we discuss tactics later in this chapter.

2.6. Data and Information

We should comment on data versus information. Information theory makes a strict distinction between information and data – that is, information is the interpretation of data by a human being. This state of affairs is comparable to information security, which also talks about information but deals with, and protects, data.

Whether this distinction does or does not make sense depends on the definition of information warfare. As seen earlier in this section, information warfare in the broader – and more accepted – sense usually overlaps with psychological and cognitive operations. In that case, it is justified to talk about information. We also have information warfare in the narrower sense, wherein whoever is applying the tactics and techniques of information warfare does not interpret the data – at least not with the intent to answer the question "why". This case is much more nuanced. Nevertheless, because the term "information warfare" is well accepted, we use it in this chapter and do not delve deeper into the question about whether it should be about data.

However, there is one interesting corner case. If an information operation tries to poison the data used to train ML models, then in this case, we are obviously dealing

13 Gelfert, 2018; Pantazi, Hale and Klein, 2021.
14 Baptista and Gradim, 2021.

with data and not information. This is just one special case and, as such, does not likely warrant a change in the accepted terminology.

2.7. Tactics, Techniques, and Sub-Techniques

Because one of our goals is to define tactics, techniques, and sub-techniques of information warfare, we must also define the meaning of these terms. One of the best databases for tactics, techniques, and sub-techniques is the MITRE ATT&CK pattern[15] for cyberwarfare. This is likely the only such database for any warfare type, and we use it as a model for building a similar database for information warfare. As already described in Section 1, the MITRE ATT&CK pattern is an extraordinarily successful database used in many situations.

The database is first divided into "tactics". For example, the tactic of "reconnaissance" encompasses all activities by the adversaries to determine as best as possible the potential target they are about to attack. Moreover, the tactic called "initial access" has the goal of entering the target network. Another tactic, "privilege escalation", is utilised while within the target network to gain appropriate privileges. Each of these tactical steps has a specific goal. Currently, there are 14 tactical steps in total, and this number changes over time. The important thing is that attackers do not have to use all the available tactical steps or follow the order listed in the database. As we already mentioned, this is not a model of attack. To conclude, tactics are defined as a reason why something is done,[16] that is, they are the objectives of the adversary.

Each tactic can be utilised in several ways, which are called techniques. Techniques are "how" the technical steps can be achieved. For example, the tactic of "initial entry" can be achieved by either exploiting a public-facing application or phishing. Some techniques can be further decomposed into more specific implementation steps, which are called sub-techniques. In the older versions of the MITRE ATT&CK pattern, they were called procedures, and the whole concept was called "Tactics, Techniques, and Procedures" (TTPs). TTP is a popular and widespread abbreviation for this concept.

The MITRE ATT&CK pattern is useful for two reasons. First, it gives defenders a catalogue of (almost) everything attackers can do (technique) to achieve something (tactic). This is invaluable to plan defences. Second, companies working on defence solutions can use this catalogue of what attackers might do to systematically cover attackers' actions in their defence solutions.

The MITRE ATT&CK pattern is developed based on what has been observed during attacks. TTPs are not the only database available in the MITRE ATT&CK pattern. It also includes a database of threats actors and the tactics and techniques

15 MITRE ATT&CK, no date.
16 Strom et al., 2020.

used by each actor. This allows for easier monitoring of threat groups. It also has a database of tools used by threat sources.

It is obvious that having similar databases for information warfare as well could be beneficial. However, the two domains are different, and the tactics and techniques for cyberwarfare cannot be expected to be easily transferred to information warfare. This chapter tries to do just that – identify the tactics and techniques of information warfare. Undoubtfully, this is just a first step, as more work is necessary to develop something for information warfare that is as useful as the MITRE ATT&CK pattern is for cyberwarfare.

2.8. ML, LLMs, and Generative AI

Research on ML is part of the bigger research area of AI. ML has been extremely popular for the past 15 years or so, mainly due to its success stories, not least of which is appearance of ChatGPT at the end of 2022. Even though ChatGPT initiated a new phase in the development and use of ML, ML already showed success in different vision and language processing tasks.

Before going further, it is necessary to provide a brief overview of AI/ML for easier understanding of the rest of this chapter. AI/ML was created for processing information in a way that is as similar as possible to how humans behave and work. Because a lot of important tasks in information warfare are performed by humans, it is obvious that replacing humans with something automated would make things more effective and efficient. Thus, AI/ML is a significant addition to the toolkit already used in information operations, as it opens up significant opportunities to make information operations even more dangerous than they are now.

First, we discuss ML models, specifically the ones based on artificial neural networks (ANNs), which are currently the most successful models. Each ANN model consists of mutually connected basic network elements, which are also connected to the outside world, to both receive data and output results. These basic network elements are called “neurons,” and each connection between two neurons transforms the information (or “signal”) that passes through it by amplifying or attenuating it. This transformation is called a parameter. In its basic form, ANN models are created according to the perception of how the human brain works at its most basic level. To conclude, each ANN model has several neurons connected in some way, and all these connections have parameters that determine what the connection will do when a signal passes through it.

Defining the exact structure of a model is an art, and the creation of different structures and use of experiments to determine which ones behave the best constitute the basic, and the hardest, part of the research in this field. The parameters, on the other hand, are defined through a process called “learning”. The learning takes input data fed into the model, and then parameters are optimised in such a way that the model produces the wanted outputs. This is a very demanding task that requires a huge amount of processing power, and huge quantities of data are also

necessary. Compared to the human brain, ANN models are significantly inefficient at learning. After the process of learning is finished, all the connections between neurons have defined values for what they should do with the signals passing through them. The number of parameters in today's state-of-the-art models are in the range of billions. In other words, there are billions of connections between neurons in one ANN model.

After the process of learning finishes, we have a trained model that can be used. Note that there is an option of so-called "pretraining", meaning that someone who creates a model does initial training with huge amounts of data, and then the user must do "finetuning", that is, training using a smaller set of domain-specific data. Even though pretraining widens the number of those who can create their own custom models, it is still resource demanding.

In the case of information operations, we are particularly interested in two classes of ML models: LLMs and deep generative models. LLMs have the specific purpose of manipulating the natural language, while deep generative models are used to create so-called "deepfakes", which are images or videos that show events or persons that do not exist.

Creating an LLM is not an easy task, and it can incur substantial cost.[17] To create an LLM from scratch, the following resources must be available: (1) AI/ML experts who will create and train models; (2) data on which models will be trained and people to collect and purify the data; (3) infrastructure for training and data collection, as well as experts that will build and maintain this infrastructure; (4) management structure to organise and oversee everything; and finally, (5) financial resources to cover operational costs.

Note that there is a plethora of LLMs currently available for different purposes. The key distinction is whether they are proprietary or so-called "open source". Proprietary models are closely guarded by their owners and are either not accessible or accessible only under certain conditions. In any case, such models run on the owner's hardware and are accessed by users via application programming interfaces (APIs) or web browsers. Moreover, the LLMs' parameters and structure are closely guarded business secrets. In general, these models are of better quality, and their prime examples are OpenAI's ChatGPT and Google's Gemini, formerly known as Bard.

Open-source models, on the other hand, are freely available for anyone to use, and there is even a centralised repository of such models.[18] Some of them come remarkably close to proprietary models because of their performance. These models can be downloaded locally and run on a local machine. Although these models require stronger hardware due to their size (number of neurons and parameters), they are still not so inaccessible to someone with enough financial resources.

The accessibility of advanced models, no matter if they are closed- or open-source, represents a significant shift in information warfare. There are already

17 Musser, 2023.
18 Hugging Face, no date.

known cases of attackers using LLMs and generative deep models either to increase the success of their attacks or as a tool of attack.[19] Research also shows that the Internet already has abundant LLM-generated content,[20] and deep fakes are already used for disinformation.[21]

2.9. Related Work

This work is certainly not the first one to use the MITRE ATT&CK pattern as a model to create a framework for information warfare. The most advanced such framework is the Disinformation Analysis and Risk Management (DISARM) framework.[22] Because DISARM is the most comprehensive framework and is also supported by the European Union and North Atlantic Treaty Organization (NATO), we compare our framework to DISARM.

The motive for creating DISARM was the same as ours: to organise and structure information operations so that defenders can be more efficient in detecting, predicting, and combating information operations. However, DISARM is much broader in scope and more encompassing.

The DISARM framework tries to combine the tactics and techniques of all warfare types enumerated in Section 2.2. For that reason, it is a flat and very complex model. However, our approach is completely different. We accept that there are different forms of warfare, each with its own specifics, which require expertise that a single person cannot have. Furthermore, we believe these forms can interact in different ways. Therefore, we tried to keep all these warfare types separate while proposing a way in which they interact by utilising the "uses" and "used by" verbs. Because this chapter emphasises information warfare, we placed it in the centre and analysed how other warfare types can use or be used by it. Thus, we created a system that has a limited set of tactics and techniques, which can be combined in complex ways. The DISARM framework, on the other hand, simplifies interactions between different warfare types by combining them and imposing a rigid structure on the result.

The DISARM framework was tested by Newman et. al. for its suitability for rapid adoption by strategic communications practitioners along with its credibility among specialist foreign information manipulation and interference threat analysts.[23] The result was positive and found DISARM to be applicable and well suited for these purposes. Operation Ghostwriter was used for testing. However, the main narrative of this operation is the heavy use of offensive cyber-capabilities to spread disinformation. We find this to be overly restrictive, as cyberoperations are not the only means of spreading disinformation. As described in Section 5.5, we consider

19 Mascellino, 2023; Hill, 2023; Chilton, 2023.
20 Cantor, 2023; Ryan-Mosley, 2023.
21 Satariano and Mozur, 2023; Philmlee, 2023.
22 *DISARM Foundation*, 2024; Terp and Breuer, 2022; López, Pastor-Galindo and Ruipérez-Valiente, 2024.
23 Newman, 2022.

cyberoperations as a means to achieve a specific position from which some goals can be achieved. As such, cyberoperations are opaque from the information warfare perspective and encapsulate complex processes that are dealt with by cybersecurity. This, again, is in line with our approach of not grouping different warfare types into a single set of tactics and techniques.

One additional restriction of the DISARM framework, which we do not have, is that it is restricted to online means of managing disinformation.[24] While most of today's information operations are conducted in the online world, traditional means are still used, especially when threat actors are nation states.

In conclusion, the DISARM framework uses a different approach to model information operations, and we offer an alternative approach. However, because DISARM is more developed with the investment of multiple manhours, it can be source of inspiration for further development of the model presented in this chapter.

Another related work is a paper presented at the 2023 Network and Distributed System Security Symposium by Shujaat et al.[25] This work deals with threats and the tactics used by threats, which makes it overlap with both our work and the DISARM framework. The value of Shujaat et al.'s work is in its threat source analysis and classification, which complements our work. However, different from our work, Shujaat et al. conflate the terms "campaign" and "operation," while we consider campaigns as consisting of multiple operations. They also treat everything as misinformation and build disinformation operations on spreading misinformation, which they call "misinformation incidents" or occurrences of misinformation. Moreover, like the DISARM framework, they heavily integrate cybersecurity tactics and techniques into the tactics and techniques for handing disinformation, while we try to keep them separate.

3. Information Operations

In this chapter, we go deeper into information operations and the environment in which they are run. We also indicate the relation between information warfare and other types of warfare. Finally, we discuss elements of information space. We start with a discussion of operational domains based on the definitions of the US Joint Forces Command and NATO, which are utilised by almost all other Western militaries.

24 Terp and Breuer, 2022.
25 Shujaat, 2023.

3.1. Operational Domains and Their Layers

The "operational domain" is where combat and military operations take place. According to the definition by the US Joint Forces Command and NATO, there are five domains of war: land, sea, air, space, and cyber. Information operations do not have their own separate domain but are interleaved with all domains because all of them are dependent on information, which is used for decision-making. Cyberspace, the fifth domain, and its relation to information operations are especially interesting. Cyberspace is conceptualised as having three layers – physical, logical, and social.[26] This layering fits nicely with our discussion of information being perceived (people having direct contact with the physical layer) and received (people receiving information through the logical network layer).

In the end, people base their decisions and actions on information, which is perceived directly or indirectly, and so this layer covers both the physical and logical network layers. Yet, as discussed in Section 2, the logical network layer is where most of the information warfare occurs, so it is of greater interest to us.

We might even extend this idea to other domains and say that all domains have always had an information layer between people and the domain in question. Furthermore, this information space stretches between different domains. This conceptual image is important because it shows where information warfare fits, as well as its primary purpose, which is to distort the reality for persons operating in different domains. It also allows the fitting of different warfare activities. We can thus conclude that "information warfare" is a form of a war waged in the "information space", and the information space fits between all operational domains and people.

3.2. Information Lifecycle

Information has a lifecycle, starting from the point it is conceived and created and ending when it is consumed. Creation and consumption happen in the persona layer of the model we described in the subsection 3.1, while everything else happens in the information space. Physical transmission, storage, and processing of information occur in the operational domains. The information lifecycle has six phases. Note that this is the most general model, and some specific means (techniques) will fuse multiple phases into one.

First, information is "created" (first phase). This is a creative process governed by the purpose for which the information is created, and this activity is part of the "persona" layer. The result of this process can have different forms – such as directions, claims to be made, and raw articles – many of which might not be appropriate for direct consumption by intended targets. This step of creating information is outside of the scope of information operations as it is tightly bound to the purpose and goals for which the information is created; as such, it is under the auspices

26 Joint Chiefs of Staff, 2018.

of psychological, cognitive, and other operations, as we explain in the following subsection.

The next step is "generating" information (second phase). This step can be automated or manual. In any case, the goal is to have variations of the original information that was created, each distinct from the others. Yet, all variations are still in the spirit of the original information, as they keep the key elements same across all variations. While manual creation is important, we are primarily interested in automated ways of generating variations.

After information is generated, the next step is "production" (third phase), wherein information is prepared for the media in which it will be published. This means that a visual representation is created for all variations.

Then, information is "published" (fourth phase). Publication could be in the form of a web page, an article in a printed copy of a newspaper, a book, etc.

After being published, information is "disseminated" (fifth phase). Based on the publication form, the information can be distributed in different ways, such as in email messages or on social media via the sharing functionality. Additionally, if someone else takes the information and shares or publishes it somewhere else, we also treat this as dissemination. There are means to get people to notice information being published and disseminate it further. For example, this can be done by placing advertisements (ads), planting links in different forums, search engine optimisation poisoning, sending mail notifications, etc. We also treat this as a form of dissemination.

Finally, information is "consumed" by targets (sixth phase), which can also trigger the process of information creation in certain cases, for example, in forums or on chat applications. Consumption is a psychological process and is again outside the scope of information warfare.

Now, we will define each step of the information lifecycle, starting from generation up to dissemination, as a "tactical step" used in information operations. Thus, we have four tactical steps – generation, production, publication, and dissemination – and we will define techniques and sub-techniques that can be used to implement each of these.

3.3. Information Forms

Information can come in many forms, the most common form being text. However, this is not the only possible or even the best form. The text form is popular because it is easy to manipulate. Other forms of information include photo, video, and audio, which were once harder to manipulate. Yet, it does not mean that these forms were not produced or manipulated, but that such manipulation occurred less frequently. Because of ML advances, such forms are increasingly being used. Some forms can be divided further into subtypes. In information warfare, disinformation that should be conveyed to targets for consumption is encoded into one of the given forms.

Before the advent of digital technologies, manipulation of information forms was a very resource- and time-consuming task. Today, however, a multitude of tools are available for this purpose, and it is much easier to produce information in different forms. Still, some forms are easier to manipulate, while others are harder. This leads the forms that are harder to manipulate to be more trustworthy, and those that are easier to manipulate to be less trustworthy. The difficulty in manipulating each information form also depends on the desired change: minor changes are easier than creating the form from scratch.

As mentioned, the easiest form to manipulate is text, especially since computers became widely available, because they allow text to be very quickly typed, copied, multiplied, etc. No matter what needs to be done, it is technically easy, be it creating text from scratch, removing certain parts from the existing text, adding parts that were not present, or modifying existing parts.

Photos are next in terms of difficulty to manipulate. They are harder to manipulate than text, but it depends on the exact modification. It is well known that many people use different applications to improve their posture in photos, but these are simple manipulations achieved by applying filters. Much harder manipulations include photo montages that might require professionals. Such manipulations by professionals might be extremely hard to detect or to prove that the photo is counterfeit or manipulated in some way. The tool professionals use most frequently for this purpose is Adobe Photoshop. Note that photo manipulation has been done almost since the advent of photography.

Videos are even harder to manipulate. It involves the manipulation of a large number of still images (equivalent to photographs), which makes video manipulation much more resource demanding than photo manipulation. Thus, it is generally restricted to simple manipulations, such as blurring specific parts of videos so something is hidden. Videos are frequently accompanied by audio, especially if they show someone talking.

Audio can be manipulated as well. Today, it is extremely easy to record any conversation, because a recorder is available in all mobile phones. This means that it is easy to convince someone that an audio recording is genuine. In other words, it is not unexpected to have an audio recording because of the prevalence of audio recorder devices.

In the tactical step of information generation, it is possible for information in one form to be transformed into another form, possibly using ML techniques.

3.4. Information Operations in Relation to Other Types of Operations

As seen in Section 2, there are several types of warfare and thus operation types. Our central theme is information warfare or information operations, and we are interested in the relationship between information warfare and other types of warfare. In the subsection 3.2 we argued that information operations deal with the process of generating information based on requirements, publishing it, and finally distributing

it. The requirements are specified by an outside process, which depends on the goals of an outside actor. Psychological, cognitive, economic, financial, political and propaganda operations dictate the requirements of information operations. All these operations have the specific goal of impacting people, the society, or some groups in between. As such, they are in a much better position to determine the best course of action.

For example, let us assume that someone is conducting a psychological operation that has as the goal of creating uncertainty and anxiety in the population, for whatever purposes it might serve. This end-state can be achieved using psychological operations in several ways. Each approach is grounded in the knowledge of psychology, which, based on human behaviour patterns, dictates what should be done to achieve the operational goals. One approach might be to have military exercises along the border of the target country, and another might be to have a military parade and boast one's superiority over the target country's military forces. Yet, the approach we are interested in the most is using information operations to spread psychological messages to the target country's population. In this case, the psychological operation gives directions on what should be spread, which is then taken by the information operation operator, adjusted for different information channels, and then published and distributed using those channels. In essence, information warfare is a tactic of psychological warfare.

Three relations between information warfare and other warfare types can be analysed. The first is when information warfare is "used by" some other warfare type. This is the case for psychological, cognitive, economic, financial, propaganda, political warfare. In this case, information operation is just one tactical or technical step for those warfare types. The second relationship is when information warfare uses some other warfare type. This is the case for cyber warfare, electronic warfare, social network warfare, and ad operations. Note that here we have, not so common, social network and ad warfare. The reason they are denoted as such is that they are quite complex activities and thus have non-trivial tactics and techniques. After all, there are many companies offering PR and marketing services, so this is a very developed activity which can be abused as well. Finally, the third relationship is subset of information warfare. For example, if we are talking about fake news and the way it could be spread, then this is only subset of disinformation that is handled by information warfare. Or, disinformation warfare, might also be treated as subset of information warfare because information warfare includes tactic of blocking information from spreading, which disinformation warfare – arguably – doesn't include. Note that we don't have superset relationship with information warfare, i.e. that some warfare type is superset of information warfare. The reason is that we treat information warfare as a canonical type of warfare. In other words, we could invent some warfare that will be a superset of information warfare, but we treat it as union of other warfare types or their parts (psychological, cognitive, cyber, etc.).

Cyber operations are interesting as they have a goal of bringing operators of information operation into a position to achieve some tactical step. For example,

if information operation planning decides that the best approach to spread some piece of disinformation is by some popular news portal, then it needs to be compromised in some specific manner that will allow planting of disinformation. This can be done, among other things, by means of cyber warfare. In general, all cyber operations consist of two steps, one getting into position to do something, and the other step is really doing something. This is not so visible in the case of pure cyber operations but becomes obvious in some special situations. Take as an example the attack on electrical power grid. In order to sabotage this system, it is necessary first to gain appropriate position (e.g. compromise of SCADA station), and then someone who knows how electrical power grid works has to manipulate system in such a way to destroy it. It cannot be done by the people who compromised the system as they have different expertise. Upon further analysis, it becomes clear that it is also the case in operations that are wholly contained in cyber space. For example, if attackers manage to compromise some database system, the exfiltration could be done by persons not skillful in attacking, but by someone who is good database admin, or something similar. The personnel capable of hacking might be transferred to another operation where compromise is required.

3.5. Elements of Information Space

Information exists in information space, and we define information space as a set of all the elements through which or on which information is stored, transmitted, or processed. Today, the majority of information space elements are in cyberspace, or on top of cyberspace, but there are the ones that are in the physical world as well, like traditional printed newspapers, TV, or radio. Our definition is intentionally very broad to cover all those media.

In general, what differentiates information space elements are parameters like directionality, speed of information spread, reach, and possibility of targeting. Regarding directionality, information can flow from threat source to targets, but not vice versa. For example, traditional newspapers are such a type of medium. On the other hand, there are mediums, dominantly modern ones based on information technology that allow bidirectional flow of information. Regarding the speed of information spread, we mean the time necessary for disinformation to reach intended target. Again, traditional media are much slower than modern ones based on information technology. The parameter of reach determines how large is the audience reached by disinformation. Newspapers, as a traditional media, have a broad reach, as well as television and radio. Modern means of communication are not so broad, unless we count traditional newspapers published on web portals. Finally, targeting is the ability to deliver disinformation to a specific group. Traditional media is again in this respect much more restricted than modern media, but it should not be underestimated. For example, there are television broadcasters followed by people that identify with the political tone of the broadcaster. Yet, this targeting is much more versatile in the case of new media based on information technology.

In the following sections we'll survey key elements of information space and give some basic characteristics of each one of them.

3.5.1. Social Media

Social media platforms are technical infrastructures supporting social networks. Social networks, on the contrary, are networks consisting of connected human beings that communicate. Many social media platform types and specific instances exist. In this section, we go over key characteristics of the more important platforms: X (formerly Twitter), Facebook, LinkedIn, Instagram, YouTube, and others.

In essence, a social media platform is more valuable the more users it has. Thus, the primary goal of all social media platforms is to attract and retain as many users as possible. The platforms are constantly changing as new services are introduced and old ones are removed. This is done to offer users a better experience and reasons to stay on the platform. Although the number of users is an important parameter, in general, it is difficult for outside observers to assess the number of users of social media platforms. These platforms do publish some numbers for marketing purposes – but they are difficult to verify. Additionally, social media platform owners find it tough to estimate the number of users because of "bots", which are software pretending to be human users that engage in different activities on a social network.

All social media platforms have similar functionality. They allow each user to publish information, and this information is shown to everyone or only to a specific group of users – depending on the method of publication and privacy settings. Published information can be shared by other users using different mechanisms. This propagates information to users that are not in direct contact with the originator of the information. Furthermore, they allow the formation of interest groups and sharing of information only within those groups. Each group can be private or public. Only members can see the content shared within private groups' networks.

Finally, almost all social media can convey all forms of information, even though some are more specialised, such as YouTube for video, Instagram for photos, and TikTok for short videos. All platforms also use some form of advertising for monetisation.

3.5.1.1. X (Formerly Twitter)

X, formerly known as Twitter, is a very influential social media with around 368 million monthly active users as of December 2022.[27] The main feature of X is the users' ability to publish messages, called "tweets", of maximum 280 characters, which replaced the previous limit of 140 characters. On 28 October 2022, Elon Musk bought Twitter and has radically changed the company since then.[28] One change

27 Dixon, 2023b.
28 Zahn, 2022.

was to close APIs' access to X. Researchers had used APIs to study behaviour on X, which had made X (actually Twitter) the most studied social media. In a bid to make money from X, Elon Musk also increased the tweet limit for verified accounts to 4,000 characters.

X has two operations for information publication and sharing. First, each user can follow other users on X, meaning that they will see on their homepages tweets from the users they follow. Additionally, X sends email messages with a summary of published tweets. The second operation is the so-called "retweet", which involves publishing someone else's tweet. This means that other users can post tweets to their followers, spreading the original (retweeted) tweets even further. It is obvious that the more followers a user has, the more influential he or she is. Moreover, the more times a tweet is retweeted, the more influential it is.

Finally, as regards the information lifecycle, X can be used to publish (tweet) disinformation and disseminate it by retweeting. Those who publish disinformation can expect a fast spread, as disinformation spreads faster on X than true news,[29] which makes X an effective platform for disinformation.

3.5.1.2. Facebook

Facebook is the most used social media with over 3 billion monthly users as of the second quarter of 2023;[30] it is also much more versatile than X. As such, it is a very influential social media platform.

There are two main concepts in Facebook. The first one is a "wall". A wall is the place, or page, where a user's activities are published for others to see. The owner of the wall can communicate publicly with other users using the wall: other users can write messages on the wall, and the owner can reply to them. All these messages are publicly visible, although privacy settings can limit visibility. The second concept is the "timeline" (previously, the news feed), which is the user's private page where the user is notified about happenings on Facebook. Because a lot of activities are going on, especially for users who have a large number of friends and/or follow many different pages, only a subset of the activities is shown. The activities to be shown are selected by an algorithm, which is not known publicly.[31]

Facebook has three operations for information publication and sharing. The first one involves becoming friends with other users on Facebook and forming a network of friends. This mechanism was intended to map friend connections from the real world, but it has diverged in the virtual world because of two reasons. First, people get to know and connect with other people through purely online means, without ever meeting in person. Second, it is questionable how strict Facebook users are about not accepting friend requests from people they do not know. Additionally,

29 Langin, 2018.
30 Statista, no date b.
31 Eslami et al., 2015.

Facebook constantly tries to detect people someone might know and offers an option to connect as friends. This detection algorithm is not perfect, and thus suggestions are offered to add completely unknown people as friends.

As in the case of X, when someone publishes a post on Facebook, it is shown on the timeline of friends. Each friend has the option of "sharing" a post, that is, showing it to his/her friends, and so on. This allows the post to reach even more users, just as in the case of X.

Because there is a limit on how many friends you might have, the second method of information sharing is "following" someone's page. That is, someone creates a page about something, and then users interested in the topic of this page can follow it. Following means having a higher chance of getting notifications in the timeline (news feed) about changes on the followed pages. The third way to connect is using "groups". Groups are created around a topic, and anyone interested in that topic can join the group. Groups can be private or public, searchable or not. Activities of public groups are visible to anyone, while private groups are only accessible to members. Searchable groups can be found by using the Facebook search functionality. In any case, membership can be controlled by group administrators, meaning that they have the full discretionary right to admit someone to the group or refuse membership.

From the perspective of the information lifecycle, it is obvious that Facebook can be used similar to X to publish and disseminate disinformation.

However, unlike X, Facebook allows users to market their posts to other users. This is a handy means to achieve two different goals regarding spreading disinformation: reaching new users and amplifying posts to existing users. Importantly, selection of users to whom a specific post is shown can be based on several parameters that allow precise targeting.

Facebook has advanced privacy settings that can be used to limit access to any of the three means to connect.[32] While privacy settings might restrict the reach of disinformation, it is questionable how many users change the default privacy settings.

3.5.1.3. LinkedIn

LinkedIn is quite similar in basic function to Facebook, but its primary users are professionals. They use LinkedIn to find a job, find employees, grow their professional network, connect with peers, etc. In 2022. LinkedIn had over 750 million users.[33] While Facebook had several issues with disinformation campaigns and privacy, it seems that LinkedIn has been spared from such content, at least compared to Facebook.

32 Facebook, no date.
33 Dixon, 2023a.

3.5.1.4. Instagram

Instagram is a social media for sharing photos. It is a more specialised version of Facebook. It also allows people to have followers and comment on photos. Instagram accounts can be private or public. A characteristic of Instagram is the so-called "influencers". Influencers are people who have a large number of followers and specialise in creating content. Often, these people participate in marketing activities and are not always transparent about it.

One important indicator on Instagram is "Instagram engagement", which is a measure of how much users interact with someone's content.[34] It aggregates all interactions – likes, comments, shares, and saves. In marketing, this measure determines how content resonates with users, and the higher the engagement, the more users identify with the content.

Just like other social media, Instagram can be used to publish and disseminate disinformation during information operations.

3.5.1.5. YouTube

YouTube specialises in video distribution. Due to its scalability and capacity, it is also used as a distribution platform for live streams. YouTube allows users to broadcast videos, which once only a few people could do. Several people specialised in content generation regularly publish on YouTube. Some of them are extremely popular and influential, meaning that they are influencers just like on Instagram. It is common for the same people have a presence on multiple social media platforms.

YouTube also has a recommendation algorithm that recommends users videos based on their watch history.[35] It is known that these recommender algorithms have issues; for example, they can radicalise people by offering more and more radical videos. Finally, YouTube is a marketing platform that inserts ads into video feeds, and its system determines who should see an ad depending on several parameters.

To allow viewer engagement, YouTube allows the comment and chat features to be attached to videos or live feeds. Moreover, each video can be "liked" or "disliked", and each view is counted. These parameters are then used as a popularity measure. Recommender algorithms use these parameters as well when determining what will be offered to a user to watch.

3.5.1.6. Other Social Media

There are many other social media platforms, which are constantly in flux, along with specialised platforms for specific interest groups. Gab is an example of a

34 Demeku, 2023.
35 Zhou, Khemmarat and Gao, 2010.

specialised social media.[36] Gab's social network is similar to X, as it allows all users to broadcast short messages of up to 300 characters; it also has certain features similar to Reddit, such as a voting system for content popularity. This platform has almost non-existent rules and was created in August 2016 in response to Twitter's moderation rules. Therefore, Gab has many alt-right users, conspiracy theorists, and a high volume of hate speech. This makes Gab a fertile ground for information operations.

TikTok is also an important social media platform. TikTok specialises in truly short-form videos, making this platform very popular among the younger generations. TikTok's popularity compelled already established social media platforms, such as Facebook and YouTube, to introduce similar features. TikTok has been abused for information operations, especially during the COVID-19 pandemic.[37]

The final social media platform we will mention is Reddit. Reddit has 2.203 billion monthly active users, and number of daily users reaches over 62 million.[38] Reddit is a more discussion-based social media platform where people can ask questions and discuss different topics. All discussions are organised in groups called "subreddits". Additionally, users can vote for others' posts and thus make them more visible to others. Researchers have identified subreddits that connect people who, for example, have doubts about climate change[39] or are interested in other topics. As such, Reddit can be used for publication and distribution of disinformation during information operations.

3.5.2. Digital Advertising

Digital advertising is a source of revenue for a large ecosystem of companies, starting with the biggest Internet companies such as Google and Facebook. It is projected that in 2024, the digital advertising market will reach US$740.3 billion.[40] This ecosystem consists of three groups of players.[41] The first group is "advertisers," representing those who want to advertise a service, good, idea, etc. The second is "publishers," which are entities (or web pages) visited by users. Publishers offer advertisers the opportunity to publish ads in parallel with content in which the users are interested. Publishers can be search engines, newspapers, or any other more or less popular site. Finally, "ad networks" are intermediaries between the advertisers and publishers. Their goal is to match publishers that offer places for ads to be shown and advertisers that have ads they wish to be shown.

The key to the success of digital advertising is the use of methods (algorithms) that try to show the users ads that are as close as possible to their interests at that time. For example, if a user uses a search engine such as Google to find something

36 Zannettou et al., 2018.
37 Basch et al., 2021.
38 Turner, 2024.
39 Kim, Stringhini and Vodenska, 2023.
40 *Statista*, no date.
41 Chen et al., 2016; Grover, 2023.

about global warming, it is possible to inject ads in the results that promote conspiracy theories about global warming. It is also possible to insert other conspiracy theories under the assumption that this person is susceptible to such disinformation. Additionally, it is possible to link ads to the geographic location of the user, which also promotes targeting. In general, ad campaigns are run by marketing and public relations agencies. These agencies offer the service of promoting goods, services, and ideas, and in doing so, they use other methods besides ads.

It is already known that certain agencies try to spread disinformation for their clients.[42] What makes this situation even worse is that these clients can deny involvement. Moreover, it is already known that cybercriminals abuse ad networks for their nefarious purposes.[43]

In conclusion, digital advertising is a great technique to implement dissemination tactics phase of the information lifecycle.

3.5.3. Communication Platforms

While communication platforms are a subset of social media, we treat them separately due to their different nature. They operate more as distribution lists, wherein information is pushed to each member of a group. This is unlike social media platforms that generally utilise a pull model of communication, wherein each user must open a specific page and fetch information. Additionally, communication platforms are less reliant on recommendation algorithms, because each user receives each message. The most popular communication platforms are WhatsApp, Viber, Telegram, and Signal, along with other, lesser known, platforms. All these platforms are bidirectional in nature, which means that every user can communicate with every other user. A notable feature of these platforms is the ability to create groups. That is, any user can create a group and add or invite other users to this group. The groups can be private or public, as in social networks. In addition, users in these groups can be anonymous because only phone numbers are necessary for registration, and temporary numbers are readily available without giving any personal data. In addition, some communication platforms guarantee end-to-end encryption, which means no third party can see the communication.

Forums are a special case of communication platforms. They are similar to WhatsApp, Viber, and others as they allow two-way communication and provide groups for discussions. Yet, they do not offer such a level of privacy and anonymity. The most popular forum, among others, that is used to spread disinformation is 4chan.[44] To create such a platform, it is enough to obtain free software support, such

42 Fisher, 2021.
43 *Cybercriminals are Using Paid Ads to Get to Top Cloud Provider's Customers*, 2015; Richet, 2022.
44 4chan, no date.

as through phpBB,[45] and obtain web hosting, which is quite cheap these days. The issue is how to make this platform popular enough to attract users.

A special case of forums involves services such as Disqus.[46] These services allow everyone to add a forum-based discussion with ease. This is used, for example, by newspaper portals. A forum is embedded under each article that allows users to comment on the article.

In conclusion, communication platforms can be used to publish and distribute disinformation. The reach varies based on the privacy settings and specific technology used, and it covers a wide range of options.

3.5.4. Traditional Media

Even though we live in a highly interconnected world dominated by the Internet and social media, we must not forget about traditional media such as radio, television, and newspapers. Even though these media have had to adjust to modern technologies, and some even suffered during such adjustment, they remain important enough. They are especially important for older people who have not embraced new technologies and do not use them much.

Note that traditional media are essentially one way communication – from broadcaster to audience. The reach depends on the popularity of the media and its targeted audience. The speed of information spread is relatively high for radio and television, but quite slow for newspapers. Finally, all these media have specific audience profiles based on their content and tone, as dictated by their publication desks.

Modern technologies have brought additional distribution channels to traditional media, along with a broader reach to consumers. That is, with the Internet, both radio and television have broadened their reach to, effectively, anywhere on the Earth. However, most radio and television stations are local in nature, or regional at most. Still, there are cases of a global influence by traditional media such as *Russia Today*.

3.5.5. Other

Other means of communication, which are not covered by the above categories, also allow information dissemination. Examples include leaflets, which can be distributed using different means, and billboards. The options are effectively countless.

We also did not mention other means of using the Internet to spread information. For example, nowadays it is easy and cheap to create an online news portal and to publish in general. All that is needed is a tool such as an instance of WordPress,[47]

45 phpBB, no date.
46 Disqus, no date.
47 WordPress, no date.

which can be found on the market for as low as US$3 per month.[48] Next, it is necessary to populate this instance with news and continuously add new material, while also building a community via, for example, ads or social media. Additionally, users can be engaged when visiting the portal by allowing comments and discussions on posts. The comment system is also relatively affordable, and there are many options. Dedicated platforms such as Disqus can be used, as already mentioned. It is also possible to embed the Facebook comment system on a page. Finally, one can announce a piece of news on social media platforms, such as Facebook, and use those platforms for engagement with readers.

Additional options to publish include blogs, plain web pages, etc. These options make spreading disinformation more dangerous, as there is no quality control of the material published on the Internet, and users in general are unable to critically assess the content they find while browsing the Internet.

3.6. Information Operation Goals

The purpose of each information operation is to push certain disinformation to the target audience. However, each information operation must have a goal it wants to achieve. For example, the operation's goal might be to push certain disinformation to a specific target group, or it might be to acquire new followers on social media or groups who believe in certain disinformation. Yet another information operation might be used to initiate some action from people, such as starting a protest. As a final example, the operation's goal might be to reinforce the belief of a target group in some disinformation. The goal possibilities for information operations are countless and are dictated by outside factors.

Note that there could also be "support information operations", wherein one operation tries to push some disinformation to the target group, but several additional information operations are defined to support the main endeavour and maximise the probability of success.

Information operations are generally not easy to run, and it is necessary to plan them beforehand, organise all the necessary resources to support operation, and then execute them properly while considering any unforeseen events. In conclusion, planning, organising, and executing information operations is a topic in itself that remains underexplored.

48 GreenGeeks Web Hosting, no date.

4. Tactics and Techniques

Section 3.2 Information Lifecycle indicated that information goes through certain phases, each of which is considered a tactic. Each tactical step defines the objective of an adversary. Tactics can be achieved using different techniques and sub-techniques. In this section, we will review some tactics that can be used as well as their associated techniques and sub-techniques, where sub-techniques are more specific technical steps. Note that this is not an exhaustive list of all techniques and sub-techniques, and only the frequently used and well-known techniques are mentioned. Also mentioned are techniques that have not necessarily been used but have the potential for use. It is left for future work to create a comprehensive database of techniques and sub-techniques, such as the MITRE ATT&CK pattern, and to better connect them to what has been observed to be used.

4.1. Generation

In some cases, disinformation that should be spread is given in a form not suitable for the targets' consumption, such as when only guidelines are given on what should be spread or the disinformation needs to be translated into another language. Alternatively, an information operation operator might want to use different publication venues. In this case, it would be harmful to use a single instance of disinformation as it might rouse suspicion among the targets regarding the validity of disinformation. For example, an information operation may create a single news article with the goal publishing it in as many newspapers or portals as possible to have an impact. In that case, the more the published texts differ, the more likely they are to leave the impression that they are the opinions of multiple people and thus will be more persuasive. Obviously, the original message, which is the core of the disinformation, must be preserved across all texts. Therefore, in general, it might be necessary to morph the original message while keeping the intended intent intact.

At least three techniques can be used to implement this step from the technical perspective: (1) humans can be used as content generators; (2) ML models can be used as content generators; and (3) ML models used by others can be poisoned to spread disinformation indirectly. In the following subsections, we go over each technique in more detail.

4.1.1. Humans as Content Generators

For a long time, the only means to manipulate information based on some prescription was by engaging human beings. While this is potentially flexible, it is also costly and dependent on the skills and knowledge of the people involved. In essence, you give instructions to workers on what they should promote along with a few specific pointers; then, the workers engage in generating different variations and possibly spreading those variations across information space elements. Obviously,

there are shortcomings to this approach. First, a single person has limited quantitative capacity, as he/she can produce only a limited number of pieces of information per day. Second, the quality of materials produced by a single person might not be satisfactory because all the produced information variations will be similar. Third, the cost is high. Finally, the more people know about something, the higher is the likelihood of a leak.

In any case, to be able to use this technique, you need resources such as troll armies, employees, collaborators, and people who are like-minded but otherwise unrelated to you.

4.1.2. Use of AI/ML for Generating Content

As mentioned in Section 2 Background, ML has made great progress in recent years that allows the replacement of humans in situations that were once deemed only the realm of human intelligence. As such, this area influences information operations significantly by lowering expenses and opening up new opportunities.

Information operation operators have the option to use LLMs to generate almost infinite variations of the disinformation they need, without relying too much on human resources. This increases their capabilities and the probability of the information operation's success. To implement this technique, information operation operators have several options. They can use publicly available ML models, such as ChatGPT. This approach might raise an issue for operators, as such ML models have safeguards embedded that prevent them from generating harmful content. The next option is using the so-called "open source" ML models, with an option of further finetuning them. In this case, the adversary must have built and maintained infrastructure, which should be managed using a logistical process. This is further discussed in Section 5 Logistics Support. Finally, ML models can also be built from scratch. This is the most resource-demanding approach and, due to the availability of open-source models, an unlikely one.

One additional option for information operation operators is to use cyberoperations to steal advanced ML models from their owners. Alternatively, they may compromise the access credentials of regular users, which allows the abuse of publicly available ML models.

4.1.3. Poisoning of ML Models

One technique to generate disinformation is to poison ML models. Namely, all models are trained on data collected from the Internet. The idea is to insert poisoned data into data used for learning so that the model users are given disinformation whenever they ask something in relation to the topic of the disinformation. This can be done in several ways, depending on what is under the control of or might be influenced by the adversary. This ecosystem of creating and distributing ML models grows more and more complex with time as new companies appear that offer new

services in relation to ML models. Here, we use a simplified model in which an adversary can control one of three components that comprise the lifecycle of an ML model: data, learning process, and model distribution.

If adversaries can influence the data, then the goal is to enter as much disinformation into the raw data with the hope that the model, during the process of learning, will pick it up and behave accordingly. There are several ways to achieve this, depending on the resources available to the adversary. First, adversaries can plant disinformation data at some key points on the Internet (e.g. Reddit). Note that, if this approach is taken, this becomes an information operation in itself because several tactical steps have to be performed to achieve it. Second, datasets for training can be published with disinformation covertly embedded. Due to the datasets' large sizes, it makes it difficult to check for disinformation and easy to plant it. Collecting training data is hard and highly resource intensive. This makes publicly available datasets valuable and commonly used. Additionally, these issues have led to companies offering data manipulation services.[49] Note that the existence of such companies adds an additional opportunity, as they are potentially weak points that can be attacked using cyberspace or other warfare operations to plant disinformation.

We end the discussion on the adversary controlling data by noting that "data missing" can also be a way to spread disinformation. By removing data that supports truth, the model can learn to spread disinformation indirectly.

The next step in ML models' lifecycle is the learning process. If an adversary can influence the learning process, he can inject disinformation during this process or even manipulate the learning process itself. The easiest way of achieving this is using cyberspace operations to infiltrate companies that train LLMs.

Alternatively, due to the popularity and demand for open-source LLMs, it is possible for an adversary to train LLMs with embedded disinformation, which is then given to everyone to use freely. However, due to resource demands, this is an unlikely option.

Finally, if an adversary controls or has influence over the distribution channel, he/she can plant poisoned models. For example, HuggingFace[50] is a very popular distribution site for different ML models, and existing cases show that it is a real threat.[51] Using cyberspace operations, it might be possible to compromise the site and plant some models on it.

4.2. Production

The goal of the production tactical step is to adjust generated content to specific media. For example, raw text might need to be formatted to fit the visuals of a portal, or text-only information might need to be complemented with pictures or

49 Toloka, no date.
50 HuggingFace, no date.
51 Lakshmanan, 2024.

transformed completely into pictures and video. The key difference between this and the previous step is that information is only transformed in this step – that is, its appearance is changed – but otherwise it stays the same.

Several technical steps can be used to implement this tactical step. First, as always, humans can be used. For example, a journalist is given a text to publish, and she might need to transform this information into a form suitable for publication in the journal she is working for. Likewise, the information needs to be converted into segments for a local television station. In these examples, the persons engaging in production might or might not know that they are spreading disinformation.

Second, some automation processes might be used. Certain transformations can be done relatively easily using simple processing means. For example, a given text to be published may need a heading and footer, which can be added easily. After all, many web pages – such as The New York Times, The Guardian, eBay, and Amazon – use this mechanism to achieve consistency and improve the readability of the content for the users.

The third approach is to use ML models. More complex processing, especially transformation of information from one form to another or augmentation of one form with another, once fell exclusively in the domain of humans. However, ML models, specifically generative ML models, show great promise in this regard. A day may come when all the user needs to tell a machine is to, for example, "[t]ake this text and make it look like it was published on by *The New York Times*", and the machine will do the rest.

We can consider fake news as being a combination of content that should be communicated to targets and a form that makes this fake news more appealing. This is because people believe it was published by a reputable source – even without checking the source. To conclude, fake news is created as a combination of two tactical steps, generation and production, and as such, multiple techniques can be used to create fake news.

4.3. Publication

Publication is the process of making a specific instance of disinformation available to people or groups targeted by the information operation. This is probably one of the richest tactical steps, along with dissemination, as regards the number of available techniques. That is, abundant techniques can be used to implement this step, including publication on social media, publication through communication platforms, publication on compromised web sites, publication through traditional communication media (radio, television, and printed newspapers), starting of rumours, use of chatbots to spread disinformation, and use of "useful idiots" to inject disinformation.[52]

52 Thrush and Feuer, 2024.

In the following subsections, we discuss some of these techniques in more detail based on the information space elements they use for publication.

4.3.1. Social Media

Social media are likely the most prominent means of publishing disinformation. The additional benefit of social media is the possibility of acquiring new supporters, as anyone can see or share a post. Moreover, social media allow targeting based on demographic and other parameters. Sub-techniques that could be used here include operators publishing information in groups on social media or on highly connected users' profiles; troll armies pushing disinformation via their social media accounts; social network bots pushing disinformation; proxies being used to push disinformation; and using cyberoperations to compromise specific users or a social media platform as a whole.

4.3.2. Communication Platforms

Communication platforms are more closed off than social media platforms, and thus they can be used primarily to reinforce the beliefs of those who already believe in a disinformation. Obviously, to be able to publish on those platforms, an agent as well as a member of the targeted group must be present on those platforms.

Again, the same sub-techniques for social media can be used for communication platforms.

4.3.3. Traditional Media

Many sub-techniques can be used to publish in traditional media: owning traditional media nd using it for publishing disinformation, sending a letter to the editorial office by pretending to be a whistle-blower, using cyberspace operations to create the possibility of injecting disinformation within other published information, sending press releases, and bribing journalists to publish some information.

4.4. Dissemination

Dissemination is the process by which published information is pushed to users that did not directly receive that information. This is another rich tactical step as regards the number of available techniques, besides the publication tactical step.

This tactical step exists to reach a broader public with disinformation that is not possible with just the publication step. For example, when something is published on Facebook, friends and followers of the person publishing might not see the message because their newsfeeds might be overwhelmed with posts from other users. The process of dissemination aims to solve this and many other issues so that information is shared widely to reach as many users within the targeted group as possible.

The following techniques can be used for the dissemination tactic. The first technique is "sharing", All social networks support some form of sharing. The potential problem with sharing is that it is not under the control of the one who published the information, and thus the operator must rely on luck in this case. Some sub-techniques might be used to persuade people to share information. The second technique is "digital advertising." By using ad networks, or ads, it is possible to push notifications about disinformation to people to whom the operator is not directly related. Furthermore, it is possible to target specific geographies, demographic characteristics, etc., as discussed in Section 2 Background. Third, it is possible to perform "advertising via proxies". In this case, the information operation operator uses proxies, as a friendly force, to push the ad instead of the operator itself. Proxies might knowingly or unknowingly participate in pushing disinformation. Good proxies that have a wide reach include influencers on social media. The fourth technique is "recommender algorithm manipulation". As we said, not all users may see the published information in certain cases. For example, on Facebook, an algorithm determines what will appear in a user's feed. In this case, manipulation is necessary for the news to be pushed high in other users' feeds.

These techniques can be further amplified and supported using troll armies, social media bots, proxies, and botnets. We further describe these in Section 5 Logistics Support.

4.5. Attenuating the Information Spread

Section 3.2 Information Lifecycle showed the phases (dis)information goes through from the point it is conceived until it is consumed by targets. However, it is also important to consider the case when information does not reach people. The tactic of "attenuating information spread" is used to prevent targets from receiving valid information that will counter the disinformation campaign. Suppressing the truth from reaching people and serving them disinformation first might have an anchoring effect on the targets.

One technique to implement this tactic is the use of cyberspace operations to prevent information flow. The easiest operation is to conduct a denial-of-service attack on the source that tries to fight disinformation. Alternatively, troll armies can be used to cast doubt on truthful information by bombarding people with questions and statements that sow uncertainty and doubt. Electromagnetic warfare can also be used to disrupt communication. These are just some examples of techniques that can be used, but there are others as well.

5. Logistics Support

Support for certain technical steps must be prepared in advance so it is available to the information operation operator. These elements can be prepared specifically for certain operations, shared between different information operations, or rented from third-party providers. The key point is that all such steps require significant resources and time to establish while also incurring maintenance costs. In this section, we review some support elements for information operations.

5.1. Troll Armies

Troll armies comprise people that either willingly or unwillingly participate in actions that aim to spread disinformation. They can be under a single command as employees of a company, such as in the case of the Internet Research Agency,[53] and they can also be distributed and loosely controlled,[54] often recruited by bribing different, unrelated people.

There are many potential usages of troll armies. They can engage in discussions related to a topic of interest for the information operation operator; they can poke around and push their agenda; or they can be used to disable or slow down the spread of information using fear, uncertainty, and doubt techniques to suppress the dissemination of true information and cast doubt on it among the targets.

Troll armies also engage in creating social media accounts and building their reputation so that they can be more persuasive when they are used.

5.2. Social Media Bots

Social media bots[55] are programs that imitate human online behaviour. They are either autonomous or semiautonomous. The advantage of social media bots is that it is much easier to create a large number of artificial users and control them. Their functionality and complexity can vary from simple activities such as liking posts or sharing them to complex interactions with humans. For example, researchers have shown how using social media bots allowed them to infiltrate the users of different organisations.[56] The advent of LLMs has opened up further possibilities. Note that certain companies also create and sell large social bots. The first such company to be exposed was Devumi.[57]

53 Bastos and Farkas, 2019.
54 Aro, 2016.
55 Chang et al., 2021; Oentaryo et al., 2016.
56 Elyashar et al., 2013.
57 Confessore, 2018.

5.3. Interest Groups

Certain information space elements support the concept of groups, which might be created naturally and in a self-organised fashion. As this does not allow any control over the process, another controllable approach needs to be used.

The controllable approach may involve a group being built in a specific time, around a common theme, and grown to be of a specific size by someone who leads the process. This group would then be used to disseminate disinformation and be abused to spread this disinformation even further.

During the build-up, other techniques might be used to speed up the process. To overcome the chicken-and-egg problem – the problem of users having no incentive to join the small group – troll armies or social media bots might be used to artificially inflate the number of group users and make it more attractive. Additionally, information about the group might be spread using, for example, ad services and troll armies, to get more people on board.

5.4. Proxies

Proxies are news outlets, groups, or individuals who push someone's agenda, but without being involved in its fabrication. In other words, they believe in the disinformation they are spreading, potentially making this misinformation. However, as discussed in Section 2 Background, we do not differentiate between disinformation and misinformation, as it requires analysing motives, which is very difficult.

Of all the proxies, certain types have great potential to spread disinformation. One such group is the so-called influencers,[58] or people with a large number of followers on social media. Influencers are just one form of celebrities, which are as old as the human society. All influencers are ready to promote products, services, or ideas in exchange for monetary compensation. They are especially dangerous if they are malleable to disinformation, truly believe in it, or do not have any moral or ethical standards. Moreover, many of today's influencers are relatively young people in their early 20s, meaning that they are inexperienced and not yet fully mature. Furthermore, many celebrities in the past openly supported certain ideas, such as political, ecological, or humanitarian ideas. Therefore, it is easy to see that they can and will be used to promote disinformation.

Another type of proxies is groups on social media that connect people with similar thinking and might be susceptible to disinformation. If a large number of members of such groups accept certain disinformation, it might start to amplify, attract other members, and start to spread outside the group.

58 Gómez, 2019.

5.5. Cyberoperations

Disinformation might also be published using cyberoperations. As argued in Section 3.4 Information Operations in Relation to Other Types of Operations, cyberoperations allow one to be in the position to take actions that are not strictly part of the cyberoperations or cyberspace in general. For example, in the case of operational technology, reaching control stations (e.g. SCADA) might allow attackers to act in the physical world – which is not in the cyber domain. For information operations, cyberspace operations could use the following sub-techniques: (1) compromise news portals, which will allow the information operation operator to engage in unauthorised publication of disinformation or change existing content and (2) compromise potentially large number of web sites, which will allow the information operation operator to publish disinformation on these sites. These sub-techniques will have effects, such as search engines rating this content higher and more users being exposed to it. Cyberspace operations are used to create and maintain botnets, which can be used for many purposes, such as mass mailing, hosting social bots,[59] generating artificial traffic, and penetrating social media or communication platforms to push disinformation.

It is noteworthy to stress the connection between three stakeholders that might cooperate or just use each other's resources. These stakeholders include (1) the nation state that potentially runs the information operation, (2) cybercriminals who have infrastructure for cyberattacks, and (3) private companies that work in the grey area of the legal framework. It is well known that the Russian state does not prosecute cybercriminals in Russia, provided that they do not attack domestically.[60] Rather, Russia actively uses cybercriminals' resources and capabilities for its state objectives.[61] Recently, connections between Chinese government institutions and private companies doing hacking-for-hire were exposed through a large data leak from the company I-Soon.[62]

All this makes cyberoperations a valuable support tool for executing information operations. Yet, as cyberoperations can do much more than that, they are a topic in themselves and are covered by dedicated chapters in this book.

5.6. News Outlets

Traditional media continue getting stronger globally, and having such outlets under direct or indirect control is valuable for spreading disinformation. There are three main types of new outlets. The first and the most influential are television networks. The second are radio stations, followed by printed newspapers. All three can

59 Greig, 2022.
60 Maurer, 2018.
61 Insikt Group, 2021.
62 Hawkins, 2024.

use the Internet to reach a broader viewership, but they dominantly operate using traditional distribution methods. This also distinguishes them from Internet-only media. Television and radio are special as they require a licence to broadcast on certain frequencies. The alternative is using satellite to reach an even broader audience.

Establishing television networks with a global reach is an expensive investment, but it is a valuable tool for nation states aspiring to become global forces to spread their influence. The most prominent example in this case is RT, previously known as *Russia Today*, an outlet for spreading Russian disinformation. More common are smaller regional and local television stations. To increase their influence and prospect of surviving, these stations might cooperate or grow through mergers and acquisitions. This way, they can become quite influential, but without proper oversight.[63]

5.7. Marketing Campaigns Support Services

Marketing is a very old discipline and currently a multi-billion-dollar industry, meaning that it has accumulated a great deal of knowledge. Moreover, the market for support activities is quite vibrant. Modern marketing heavily relies on the Internet, particularly social media. Because information operations can be seen as a form of marketing, much of the marketing knowledge and even support tools can be abused for information operations. Tools developed for marketing campaigns can also be abused for information operations.

Malicious users can develop their own tools or use already existing tools, which is much easier. According to the Gartner Magic Quadrant for B2B Marketing Automation Platforms,[64] the leaders in marketing automation platforms are Adobe, Oracle, Salesforce, HubSpot, and Creatio. The key characteristic of marketing automation platforms is their ability to seamlessly integrate different social media platforms and make it much easier to have a presence on all of them.

5.8. Environment to Run ML Models

The final important logistical support is the environment for running ML models. With the increasing capability of ML models and their potential in information warfare, it is expected that their use will increase. Therefore, it is necessary to have an appropriate environment to run the models. In essence, it is necessary to have compute resources, and there are multitude of options for obtaining such resources.

The first option is using commercially available ML models such as ChatGPT. These models are relatively cheap and offer APIs, so they can be accessed programmatically and integrated into one's own applications. On the other hand, the issue for malicious users is that owners of publicly available ML models embed safeguards

63 *Last Week Tonight with John Oliver*, 2017.
64 Wagner, 2021.

to prevent misuse and protect users. As such, those models will refuse to generate malicious content. Although these safeguards are not perfect and there are ways to circumvent them, they create an annoyance for malicious users, leading them to use other tools.

Currently, it is not known to the author of this chapter if the cybercrime underground offers the service of running ML models. However, if ML models prove useful to malicious users, there will be a demand for such models, which will provoke the supply part as well.

Another option for malicious users is to buy and use their own equipment. This can range from a single computer to a computer cluster in a dedicated room. Using this equipment, malicious users can train, finetune, and run open-source ML models. As there will be no restrictions on these models' use, they would offer the greatest flexibility with an appropriate price tag.

6. Threat Sources and Actors

Many actors see information operations as a means to achieve their goals. However, throughout much of history, the only ones who could utilise information operations were nation states. In the 20th century, a significant shift occurred as big industries with a lot of resources also started manipulating information to achieve their goals. The prime examples were the tobacco and oil industries, which respectively used scientists with questionable ethical standards to cast doubt on the health damage caused by tobacco[65] and to question research showing how climate change can impact the Earth.[66] Proliferation of the Internet and popularity of social media have caused another significant shift that opened up additional powerful avenues for manipulating public opinion. Finally, the advancement of AI will undoubtedly open up means for manipulating others to achieve some gain.

For all these reasons, the question of "who" is conducting influence operations is not so straightforward as it used to be and is thus difficult to answer. By knowing who is running the information operation, we can determine their motives, capabilities, and resources, which allows us to better protect ourselves, and vice versa. That is, if we know something about the information operation, it will allow us to deduce who is behind it and the take appropriate measures.

The terminology in this subsection is taken from cybersecurity. A "threat actor" or "threat agent" is an entity that initiates a threat:[67] it might be a human being, malware, or an AI/ML model. "Threat sources", on the other hand, are the ones

65 McKee, 2017.
66 Hulac, 2016.
67 Johnson et al., 2016.

with motive, and they control or influence threat agents. Note that it is possible for a threat agent and threat source to be the same, but they are generally separate entities. We use the following parameters to distinguish threat sources. The first is "motives", which determine why the threat source is doing something. The motive can be to gain (geo)political advantage, spread conspiracy theories because threat sources believe in them, gain competitive advantage, maintain the current market position, etc. The second parameter is "capabilities", which are the skills and knowledge of people that the threat source has at its disposal. This also includes existing material resources in the form of technology, such as computing power and AI/ML models. The final parameter is "resources", which represent everything a threat source might employ, including finance, but they take time to operationalise. Resources are also important for persistence, since without resources, capabilities cannot be sustained or expanded.

The most capable threat sources are still nation states. They have the greatest capabilities and almost unlimited resources. Their motives are mainly geopolitical. On the other end of the spectrum are groups and individuals. Their motives can be, for example, political or religious, but their resources and capabilities are not as great as that of a nation state. This does not mean that individuals and, especially, groups cannot obtain a significant number of resources. Groups can be formed from the industry, be politically motivated, etc. Moreover, they can be formal or informal. Formal groups are coordinated and have aligned motives. Informal groups, on the other hand, do not have coordination mechanisms between members, who may have widely different motives that overlap only in some parts that are common to the group.

Attribution is the process of answering the question of "who" is behind an information operation – who the threat sources and threat actors are. Attribution is a much studied problem in cybersecurity where it is considered a difficult issue for several technical and legal reasons.[68] This section presents the technical issues that make attribution a problem and show where the legal issues come into play.

Attribution can be direct or indirect. "Direct attribution" is achieved when there is a clear chain of artefacts that connect an action to a threat source or threat actor. "Indirect attribution" occurs when there is no direct sequence, but we must somehow associate two or more such sequences. In general, attribution is a probabilistic process, wherein we can attribute an action to a threat source or threat actor with certain probability.

As an example of direct attribution, let us say that a threat actor published a post in a public forum using his work machine. In that case, the forum's server logs will have an entry that contains the Internet protocol (IP) address of where the post came from, and this IP address can be specifically pinpointed to some organisation. The chain in this case consists of the post in the public forum, IP address, and information that this IP address is assigned to a specific organisation. Note that this

68 Rid and Buchanan, 2015.

is a specific case as a lot of details can break this chain. To illustrate breaking of the chain, suppose that the recorded IP address comes from a dynamically allocated range belonging to an Internet service provider (ISP) that randomly assigns them to different users for a limited amount of time. In this case, to complete the chain, we need information about "who" was using this IP address at a given time, which should be provided by the ISP. Now, here is where the legal issues come into play. To obtain information on who used the IP address, a warrant must be issued to the ISP to disclose this information to law enforcement. However, if the ISP is in another country, the process becomes slower, to a point that can become impossible to obtain the required information due to another country's unwillingness to cooperate.

The above examples used a single technical artefact (IP address) for attribution; however, generally, it is necessary to connect several technical artefacts to identify the threat actor.

Threat actors, especially the more sophisticated ones, actively try to conceal their whereabouts by using different mechanisms and techniques. First, threat actors might compromise a server on the Internet and use it as a steppingstone for the attack. In this case, what the victim can see is the IP address of a compromised host. In addition, if the threat actor used a compromised host in a country that does not want to cooperate, then the victim will not be able to obtain logs from the compromised server, and thus the threat actor's IP address will stay hidden. Additionally, there might not be any logs, they might not be kept for a sufficiently long time, or they might be erased by the threat actor. In any case, this means that it is harder or impossible to reach the threat source. There are many other variations of this theme that achieve the same goal of disrupting the chain of artefacts. Second, several approaches to conceal one's IP address are frequently used on the Internet. The first approach is the use of virtual private networks (VPNs),[69] which allow users to hide their original IP address. The problem with this approach is that the threat actor places trust in the VPN provider, which could be justified in some cases but not in others. Another approach involves using an anonymising network such as Tor.[70] When used correctly, the Tor network makes it almost impossible to find the perpetrator.

Note that the use of direct methods could reveal the threat actors but not threat sources. This should be obvious, as threat sources are the ones executing operations and thus using technical means. On the other hand, threat sources just issue orders, give directions, and are engaged in similar activities so there is no chain of artefacts linking the threat actor to the threat source.

If direct methods fail, we are left to use indirect methods. In this case, we enter into the realm of intelligence, which, by its very nature, deals with uncertainties, clues, indications, hypotheses, etc. As an example of an indirect method, suppose that some disinformation appeared. The easiest way to identify the threat source is to analyse who benefits the most from it. Yet, there is no conclusive proof, as

69 Khan et al., 2018.
70 Çalışkan, Minárik and Osula, 2015.

someone else might have initiated the disinformation for certain reasons. In other words, these methods only provide an indication. However, by accumulating indications, we increase the probability until we can treat the inference as highly likely, almost conclusive. Note that in this example, we are deducing the identity of the threat source but do not know the threat actor – unless they are the same.

Finally, it is instructive to read the 2012 blog post[71] by Sophos, which shows how it is possible to identify threat actors using only open sources on the Internet.

7. Example of the Application of Tactics and Techniques

To show how these tactics and techniques might be used, we take a well-known information operation and map it to the proposed tactics and techniques. Note that this is not meant to be a validation step, as it would require much more space than we have at our disposal. This task is left for future work.

There are several known complex information operations whose consequences are still felt. Among these is Operation Denver, an information campaign by the KGB to spread disinformation about AIDS being the product of scientific research. Moreover, denials of the global warming issue still create a lot of obstacles for actions to remedy this situation. We already mentioned the tobacco industry and its fight to prevent the prohibition of smoking. Finally, most recently, COVID-19-related disinformation made it harder to implement appropriate responses to the pandemic. These are not the only disinformation campaigns. For example, because of the current Russian aggression on Ukraine, Russia spread a lot of disinformation to try to induce disagreements and conflicts between Western countries and Ukraine to weaken support for the latter. Moreover, there is an increased level of disinformation activity during each election. Certain publicly available sites monitor disinformation as it appears and try to debunk it.[72]

Disinformation is spread in not only Europe but also Africa and other underdeveloped regions in the world where Russia and other countries fight for influence. This is a huge strategic issue because fighting disinformation "at home" has no effects on disinformation elsewhere; thus disinformation takes root in other places, making it very difficult to counteract it in the future.

Of all disinformation campaigns, we selected the oldest one, Operation Denver, to illustrate the use of tactics and techniques presented in this chapter. This operation was thoroughly analysed and is documented in great detail, making it perfect

71 Drömer and Kollberg, 2012; unfortunately, the original post is lost due to the changes to the Sophos site. The cited work is a Croatian translation, but you can use Google Translate to translate it into English or any other language.

72 EU Disinfo Lab, no date; EUvsDisinfo, no date; *Tracking Disinformation and Conflict*, no date.

for our needs in this section. This campaign is also interesting because it occurred before widespread use of the Internet and modern technologies in general, while its consequences are still felt, especially in Third World countries.

Operation Denver,[73] also known as Infektion, was a complex and elaborate campaign by the Soviet Union (threat source) in the 1980s. It used the then newly discovered human immunodeficiency virus (HIV-1) to build a public image that the virus was created in the US in secret military laboratories. Additionally, there was a complex interplay with misinformation spreading from the LGBT community in the US, and multiple threat sources and threat agents were involved. All this makes this case very hard to untangle, but our goal is to identify the information operations run by KGB (threat agent), and we will ignore all other developments, as we believe that this case also falls in the realm of psychological operations.

As already mentioned, a campaign refers to several operations that all support the end-state. The motives and goals of the HIV campaign were to[74] (1) discredit the US and generate anti-American sentiments abroad; (2) reinforce the longstanding false Soviet propaganda of biological warfare activities by the US and counter US reports of Soviet violations of the 1925 Geneva Protocol on Chemical Weapons and 1972 Biological Weapons Convention; (3) undermine US defence arrangements with allied countries and create pressures for the removal of US military facilities overseas by linking the spread of AIDS to the presence of US armed force personnel stationed abroad; and (4) discourage contacts with Americans (including tourists, diplomats, and businesspeople).

The threat source in this case was a nation state, the Soviet Union. The threat actors were the KGB, scientists, and other Eastern intelligence agencies, notably East Germany's Stasi.

From the perspective of KGB, everything started with a letter published in 1983 in the Indian newspaper *Patriot*, which was a KGB-run operation. Regarding the information lifecycle, the sequence of tactical events for this specific event (letter appearing in the newspaper) was as follows: (1) Generating information: The information purporting to come from an anonymous yet "well-known American scientist and anthropologist" in New York was created. The key points of this letter were the given "facts" – AIDS was created in a laboratory and was developed in cooperation with the US Centers for Disease Control. (2) Production: The text had to be converted into a letter form and mailed to the intended destination while ensuring that it would not be lost. (3) Publication of information: The falsified letter was published in the Indian news outlet *Patriot*. (4) Distribution of information: The initial distribution was done by *Patriot*.

The follow up operation was initiated two years after, when this disinformation was reproduced in the Soviet Union. On 30 October 1985, Soviet newspaper *Literaturnaya Gazeta*, also an outlet for spreading KGB disinformation, published an

73 Selvage, 2019; Selvage, 2021.
74 US Department of State, 1987.

article by Valentin Vasilevich Zapevalov. Zapevalov was a threat agent tasked with further spreading the disinformation published in the letter in *Patriot*.

Yet another operation was run during August and September 1986, when a photocopied brochure was handed out before, during, and after a summit meeting of the Non-Aligned Movement in Harare, Zimbabwe. The purpose of the operation was to downplay the green monkey hypothesis regarding the African origin of AIDS.

Again, if we look at the information lifecycle, the sequence of events was as follows: (1) Generating information: This step was a bit more involved as it requested the aggregation of information from several sources. The result was a text that was to be published. (2) Production: This step involved the preparation of leaflets. (3) Publication and distribution of information: In this case, the information's publication and distribution were indistinguishable.

Another operation used falsified scientific research to corroborate the initial thesis of HIV being a biological weapon created in US laboratories. The following tactical steps were used in this operation: (1) Generation: The information was generated by a corrupt scientist, Jakob Segal, who produced flawed scientific research "proving" that HIV was created in US laboratories. The input for this step was the narrative about HIV being created in secret US laboratories. (2) Production: This step was non-existent in this case as everything was done by either the person who generated the disinformation or the publication venue as part of its standard procedures. Thus, it was not under the control of an information operation operator. (3) Publication: The falsified research was published in a journal, which made it publicly available and thus increased the validity of the disinformation. (4) Dissemination: The paper was cited on different occasions and in media outlets as a reputable source to confirm the initial thesis – HIV was created in a secret US laboratory.

In conclusion, Operation Denver was a complex campaign that consisted of several operations spread over many years. The operations were run by different threat actors and threat sources, which were not all mutually coordinated, nor did they have the same motives. Nevertheless, the basic idea of HIV being produced in US biological laboratories suited all threats and was used by the threat sources for their ends, although the explanation for why it was produced differed.

8. Conclusions

Fake news and disinformation in general are significant threats to modern societies and their democracies. There are many documented cases of the negative impact of disinformation on election results, population health, etc. Efforts that try to combat the spread of disinformation exist, but they are lacking, and new approaches must be found and pursued. These approaches must come from the highest levels of political decision-making. Yet, it is difficult to create strategies to address

disinformation if there is no systematisation of disinformation activities to describe in a structured and clear way what the adversaries are doing, what they might do, and how the problem of information warfare develops over time. The goal of this chapter was to lay the foundation to solve this issue through the collaborative work of many individuals.

In the beginning, we first clarified the terminology used in this chapter. We started from the basics as there are no official standards or similar regarding the use of terminology in this area. The first contribution of this chapter is viewing information warfare and warfare in general as tactics, techniques, and sub-techniques used during information operations. We also distinguished between information warfare in the narrower and broader senses. Information warfare in the broader sense includes tactics, techniques, and procedures from psychological warfare, political warfare, propaganda warfare, and other warfare types. In this chapter, the emphasis is on information warfare in the narrower sense. Information warfare in the narrower sense does not deal with the question of why there is specific disinformation nor how it affects targets. It only deals with ways of delivering disinformation to the given targets. This approach was inspired by information security. Namely, information security deals with the security of information, but it does not try to understand the content of information or how it impacts users. So, we took the perspective that information warfare deals with how to spread disinformation, while we considered the questions of why it is created and what its psychological and other consequences are as outside the scope of information warfare.

We also dealt with information operations. We reviewed the military operational domains to determine where information warfare fits. We concluded that information warfare is embedded in all military domains as it impacts people as its final target. We also defined the information lifecycle by defining the four phases of generation, production, publication, and dissemination. These four phases are tactical steps we later studied in more detail. We also showed that information has several forms: text, video, audio, pictures, and different combinations thereof. Finally, we analysed the information space and its main elements where information operations take place.

This chapter had the main goal of systematising activities related to information warfare in a way that allows more effective and efficient combating of adversaries who use information warfare. The main inspiration comes from the success of the MITRE ATT&CK pattern database for cyberwarfare. This database contains a list of tactics, techniques, and sub-techniques observed in the real world. It also contains a list of threat actors, along with the tactics and techniques they use. The database is used in discussions on attackers' behaviour as well as in products used for defence, and new uses are constantly being identified. Therefore, in Section 4 Tactics and Techniques, we tried to develop a similar database for information warfare. Because creating something as comprehensive as the MITRE ATT&CK pattern is a huge endeavour, the results presented here should be taken as only a first step.

Certain techniques depend on logistical support, and in Section 5 Logistics Support, we enumerated infrastructure that might be created before certain

information operations are enacted and that could be shared between several information operations. We also discussed troll armies, social media bots, interest groups, proxies, cyberoperations, news outlets, marketing campaign support services, and the environment to run ML algorithms.

Finally, we argued that there should be a taxonomy of threat actors and threat sources based on their motives, capabilities, and resources. This is important because we are no longer dealing with only nation states when talking about information warfare. Information warfare can be, and is, used by many other actors, and cataloguing them and identifying their tactics, techniques, and sub-techniques is a valuable addition to a toolbox that allows more efficient and effective suppression of disinformation.

Finally, we considered Operation Denver as an example. We described its operations and showed how the actions taken during this operation can be mapped to our proposed tactics, techniques, and sub-techniques.

In future work, this activity should be more data driven. Namely, data about information operations should be collected, and each information operation should be mapped to the proposed tactics, techniques, and sub-techniques. This mapping would generate feedback on what is good and what needs to be changed. Moreover, a database of threat actors and their activities should be created.

We believe that by expanding the work presented here, more efficient and effective policies and mechanisms can be created to combat information and disinformation operations. This will help achieve the ultimate goal of protecting modern societies and their democracies from the harm caused by disinformation.

References

4chan. (no date). [Online]. Available at: https://www.4chan.org/ (Retrieved: 15 March 2024).

Aro, J. (2016) 'The cyberspace war: propaganda and trolling as warfare tools', *European view*, 15(1), pp. 121–132; https://doi.org/10.1007/s12290-016-0395-5.

Baptista, J.P., Gradim, A. (2021) '"Brave New World" of fake news: How it works', *Javnost-the public*, 28(4), pp. 426–443; https://doi.org/10.1080/13183222.2021.1861409.

Basch, C.H., Meleo-Erwin, Z., Fera, J., Jaime, C., Basch, C.E. (2021) 'A global pandemic in the time of viral memes: COVID-19 vaccine misinformation and disinformation on TikTok', *Human Vaccines & Immunotherapeutics*, 17(8), pp. 2373–2377; https://doi.org/10.1080/21645515.2021.1894896.

Bastos, M., Farkas, J. (2019) '"Donald Trump is my President!": the Internet Research Agency propaganda machine', *Social Media+ Society*, 5(3); https://doi.org/10.1177/2056305119865466.

Çalışkan, E., Minárik, T., Osula, A.-M. (2015) *Technical and legal overview of the tor anonymity network*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. [Online]. Available at: https://www.ukita.co.uk/surveillance/2015/TOR_Anonymity_Network.pdf (Accessed: 14 March 2024).

Cantor, M. (2023) 'Nearly 50 news websites are 'AI-generated', a study says. Would I be able to tell?', *The Guardian*, 8 May 2023. [Online]. Available at: https://www.theguardian.com/technology/2023/may/08/ai-generated-news-websites-study (Accessed: 14 March 2024).

Chang, H.-C. H., Chen, E., Zhang, M., Muric, G., Ferrara, E. (2021) 'Social bots and social media manipulation in 2020: the year in review' in Engel, U., Quan-Haase, A., Liu, S., Lyberg, E.L. (eds.) *Handbook of Computational Social Science, Volume 1*. 1st edn. London, UK: Routledge; pp. 304–323; https://doi.org/10.4324/9781003024583.

Chen, G., Cox, J.H., Uluagac, A.S., Copeland, J.A. (2016) 'In-Depth Survey of Digital Advertising Technologies', *IEEE Communications Surveys & Tutorials*, 18(3), pp. 2124–2148; https://doi.org/10.1109/COMST.2016.2519912.

Chilton, J. (2023) 'The New Risks ChatGPT Poses to Cybersecurity', *Harvard Business Review*, 21 April 2023. [Online]. Available at: https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecurity (Accessed: 14 March 2024).

Confessore, N., Dance, G.J., Harris, R., Hansen, M. (2018) 'The follower factory', *The New York Times*, 27 January 2018. [Online]. Available at: https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html (Accessed: 15 March 2024).

Demeku, A. (2023) 'What You Need to Know About Your Engagement Rate on Instagram', *Later*, 14 July 2023. [Online]. Available at: https://later.com/blog/instagram-engagement-rate/ (Accessed: 16 February 2024).

Dinstein, Y. (2011) *War, aggression and self-defence*. 5th edn. Cambridge: Cambridge Univeristy Press; https://doi.org/10.1017/CBO9780511920622.

Dixon, S.J. (2023a) 'LinkedIn – Statistics & Facts', *Statista*, 12 December 2023. [Online]. Available at: https://www.statista.com/topics/951/linkedin/ (Accessed: 14 March 2024).

Dixon, S.J. (2023b) 'Number of X (formerly Twitter) users worldwide from 2019 to 2024', *Statista*, 15 November 2023. [Online]. Available at: https://www.statista.com/statistics/303681/twitter-users-worldwide/ (Accessed: 5 February 2024).

Drömer, J., Kollberg, D. (2012) 'Istraga bande iza Koobeface zloćudnog koda' [Investigation of the gang behind the Koobface malware code], *Blogspot*, 22 January 2012. [Online]. Available at: http://sgros.blogspot.com/2012/01/istraga-bande-iza-koobeface-zlocudnog.html (Accessed: 8 June 2024).

Elyashar, A., Fire, M., Kagan, D., Elovici, Y. (2013) 'Homing socialbots: intrusion on a specific organization's employee using Socialbots', *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pp. 1358–1365; https://doi.org/10.1145/2492517.2500225.

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K., Sandvig, C. (2015) '"I always assumed that I wasn't really that close to [her]": Reasoning about Invisible Algorithms in News Feeds', *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 153–162; https://doi.org/10.1145/2702123.2702556.

EU Disinfo Lab (no date) 'A Vibrant Home for Disinformation Activists and Experts'. [Online]. Available at: https://www.disinfo.eu/ (Accessed: 15 March 2024).

EUvsDisinfo (no date). [Online]. Available at: https://euvsdisinfo.eu/ (Accessed: 15 March 2024).

Facebook (no date) 'Basic Privacy Settings & Tools'. [Online]. Available at: https://www.facebook.com/help/325807937506242 (Accessed: 28 December 2023).

Farago, L. (1941) *German psychological warfare*. New York: Committee for National Morale.

Fisher, M. (2021) 'Disinformation for Hire, a Shadow Industry, Is Quietly Booming', *The New York Times*, 25 July 2021. [Online]. Available at: https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html (Accessed: 21 February 2024).

Gelfert, A. (2018) 'Fake News: A Definition', *Informal Logic*, 38(1), pp. 84–117; https://doi.org/10.22329/il.v38i1.5068.

Goldstein, J.A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., Sedova, K. (2023) 'Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations', *arXiv*, preprint arXiv:2301.04246; https://doi.org/10.48550/arXiv.2301.04246.

Gómez, A.R. (2019) 'Digital Fame and Fortune in the age of Social Media: A Classification of social media influencers', *aDResearch ESIC International Journal of Communication Research*, 19(19), pp. 8–29.

GreenGeeks Web Hosting (no date) 'WordPress Hosting – Fast, Secure & Managed by Expert 24/7 Support'. [Online]. Available at: https://www.greengeeks.com/wordpress-hosting (Accessed: 15 March 2024).

Greig, J. (2022) 'Russian government procured powerful botnet to shift social media trending topics', *The Record*, 20 May 2022. [Online]. Available at: https://therecord.media/russia-botnet-fronton-social-media-nisos (Accessed: 20 May 2022).

Grover, S. (2023) '22 Best Ad Networks for Publishers in 2023', *adpushup*, 4 May 2023. [Online]. Available at: https://www.adpushup.com/blog/the-best-ad-networks-for-publishers/ (Accessed: 11 November 2023).

Hawkins, A. (2024) 'Huge cybersecurity leak lifts lid on world of China's hackers for hire', *The Guardian*, 23 February 2024. [Online]. Available at: https://www.theguardian.com/technology/2024/feb/23/huge-cybersecurity-leak-lifts-lid-on-world-of-chinas-hackers-for-hire (Accessed: 15 March 2024).

Hill, M. (2023) '5 ways threat actors can use ChatGPT to enhance attacks', *CSO*, 28 April 2023. [Online]. Available at: https://www.csoonline.com/article/575205/5-ways-threat-actors-can-use-chatgpt-to-enhance-attacks.html (Accessed: 14 March 2024).

HuggingFace (no date) 'The AI community building the future'. [Online]. Available at: https://huggingface.co/ (Accessed: 14 March 2024).

Hulac, B. (2016) 'Tobacco and oil industries used same researchers to sway public', *Scientific American*, 20 July 2016. [Online]. Available at: https://www.scientificamerican.com/article/tobacco-and-oil-industries-used-same-researchers-to-sway-public1/ (Accessed: 15 March 2024).

Hutchins, E., Cloppert, M., Amin, R. (2011) *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Washington, DC: Academic Publishing International Limited.

Insikt Group (2021) 'Dark Covenant: Connections Between the Russian State and Criminal Actors', *Recorded Future*, 9 September 2021. [Online]. Available at: https://www.recordedfuture.com/blog/russian-state-connections-criminal-actors (Accessed: 15 March 2024).

Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C. (2016) 'Guide to Cyber Threat Information Sharing', *National Institute of Standards and Technology*, October 2016; http://dx.doi.org/10.6028/NIST.SP.800-150.

Joint Chiefs of Staff (2018) 'Cyberspace Operations', *Joint Publication 3-12*, 8 June. [Online]. Available at: https://irp.fas.org/doddir/dod/jp3_12.pdf (Accessed: 8 June 2024).

Khan, M.T., DeBlasio, J., Voelker, G.M., Snoeren, A.C., Kanich, C., Vallina-Rodriguez, N. (2018) 'An empirical analysis of the commercial VPN ecosystem', *Proceedings of the Internet Measurement Conference*, pp. 443–456; https://doi.org/10.1145/3278532.3278570.

Kim, H., Stringhini, G., Vodenska, I. (2023) 'How Climate Disinformation Spreads: Reddit', *Institute for Global Sustainability*, 31 May 2023. [Online]. Available at: https://www.bu.edu/igs/research/projects/climate-disinformation-initiative/reddit/ (Accessed: 14 March 2024).

Langin, K. (2018) 'Fake news spreads faster than true news on Twitter – thanks to people, not bots', *Science*, 8 March 2018. [Online]. Available at: https://www.science.org/content/article/fake-news-spreads-faster-true-news-twitter-thanks-people-not-bots (Accessed: 14 March 2024).

Larson, E.V., Derilek, R.E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L.H., Thurston, C.Q. (2009) *Foundations of effective influence operations: A framework for enhancing army capabilities*. Santa Monica, CA: Rand Corporation.

López, A., Pastor-Galindo, J., Ruipérez-Valiente, J.A. (2024) 'Frameworks, Modeling and Simulations of Misinformation and Disinformation: A Systematic Literature Review', *arXiv*, preprint arXiv:2406.09343.

Mascellino, A. (2023) 'New ChatGPT Attack Technique Spreads Malicious Packages', *Infosecurity Magazine*, 6 June 2023. [Online]. Available at: https://www.infosecurity-magazine.com/news/chatgpt-spreads-malicious-packages/ (Accessed: 14 March 2024).

Maurer, T. (2018) 'Why the Russian Government Turns a Blind Eye to Cybercriminals', *Slate*, 2 February 2018. [Online]. Available at: https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499 (Accessed: 15 March 2018).

McKee, M. (2017) 'The tobacco industry: the pioneer of fake news', *Journal of public health research*, 6(1); https://doi.org/10.4081/jphr.2017.878.

MITRE ATT&CK (no date). [Online]. Available at: https://attack.mitre.org/ (Accessed: 14 March 2024).

Musser, M. (2023) 'A cost analysis of generative language models and influence operations', *arXiv*. [Online]. Available at: https://arxiv.org/abs/2308.03740 (Accessed: 8 June 2024).

Newman, H. (2022) *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM' (prepared in cooperation with Hybrid COE)*. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, NATO Strategic Communications Centre of Excellence.

Oentaryo, R.J., Murdopo, A., Prasetyo, P.K., Lim, E.-P. (2016) 'On profiling bots in social media' in Spiro, E., Ahn, Y.-Y. (eds.) *International Conference on Social Informatics*. Bellevue, WA, USA: Springer International Publishing, pp. 92–109; https://doi.org/10.1007/978-3-319-47880-7_6.

Pantazi, M., Hale, S., Klein, O. (2021) 'Social and Cognitive Aspects of the Vulnerability to Political Misinformation', *Political Psychology*, 42(1), pp. 267–304; https://doi.org/10.1111/pops.12797.

Philmlee, D. (2023) 'Practice Innovations: Seeing is no longer believing – the rise of deepfakes', *Thomson Reuters*, 18 July 2023. [Online]. Available at: https://www.thomsonreuters.com/en-us/posts/technology/practice-innovations-deepfakes/ (Accessed: 14 March 2024).

phpBB (no date) *phpBB forum software*. [Online]. Available at: https://www.phpbb.com/ (Accessed: 15 March 2024).

Richet, J.-L. (2022) 'How cybercriminal communities grow and change: An investigation of ad-fraud communities', *Technological Forecasting and Social Change*, 2022/174; https://doi.org/10.1016/j.techfore.2021.121282.

Rid, T. (2012) 'Cyber war will not take place', *Journal of strategic studies*, 35(1), pp. 5–13; https://doi.org/10.1080/01402390.2011.608939.

Rid, T., Buchanan, B. (2015) 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38(1), pp. 4–37; https://doi.org/10.1080/01402390.2014.977382.

Ryan-Mosley, T. (2023) 'Junk websites filled with AI-generated text are pulling in money from programmatic ads', *MIT Technology Review*, 26 June 2023. [Online]. Available at: https://www.technologyreview.com/2023/06/26/1075504/junk-websites-filled-with-ai-generated-text-are-pulling-in-money-from-programmatic-ads/ (Accessed: 14 March 2024).

Satariano, A., Mozur, P. (2023). 'The People Onscreen Are Fake. The Disinformation Is Real', *The New York Times*, 7 February 2023. [Online]. Available at: https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html (Accessed: 14 March 2024).

Selvage, D. (2019) 'Operation "Denver": The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985–1986 (Part 1)', *Journal of Cold War Studies*, 21(4), pp. 71–123; https://doi.org/10.1162/jcws_a_00907.

Selvage, D. (2021) 'Operation "Denver" The East German Ministry for State Security and the KGB's AIDS Disinformation Campaign, 1986–1989 (Part 2)', *Journal of Cold War Studies*, 23(3), pp. 4–80; https://doi.org/10.1162/jcws_a_01024.

Shujaat, M., Labeeba, B., Liang, N., Sarah, P., Azza, A., Papotti, P., Popper, C. (2023) *Tactics, Threats & Targets: Modeling Disinformation and its Mitigation*. San Diego: Network and Distributed System Security (NDSS) Symposium.

Smith, B.L. (2024) 'propaganda', *Encyclopedia Britannica*. [Online]. Available at: https://www.britannica.com/topic/propaganda (Accessed: 19 February 2024).

Southerland, M. (2016) *China's Island Building in the South China Sea: Damage to the Marine Environment, Implications, and International Law.* Washington DC, USA: US-China Economic and Security Review Commission.

Stone, J. (2013) 'Cyber war will take place!', Jou*rnal of strategic studies*, 36(1), pp. 101–108; https://doi.org/10.1080/01402390.2012.730485.

Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B. (2020) 'MITRE ATT&CK®: Design and Philosophy', March 2020. [Online]. Available at: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (Accessed: 8 June 2024).

Terp, S.-J., Breuer, P. (2022) 'DISARM: a framework for analysis of disinformation campaigns', *2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management* (CogSIMA), pp. 1–8; https://doi.org/10.1109/CogSIMA54611.2022.9830669.

Lakshmanan, R. (2024) 'New Hugging Face Vulnerability Exposes AI Models to Supply Chain Attacks', *The Hacker News*, 27 February 2024. [Online]. Available at: https://thehackernews.com/2024/02/new-hugging-face-vulnerability-exposes.html (Accessed: 15 March 2024).

Thrush, G., Feuer, A. (2024) 'Ex-Informant Accused of Lying About Bidens Said He Had Russian Contacts', *The New York Times*, 20 February 2024. [Online]. Available at: https://www.nytimes.com/2024/02/20/us/politics/fbi-informant-hunter-biden.html (Accessed: 23 February 2024).

Toloka (no date). [Online]. Available at: https://toloka.ai/data-labeling-platform/ (Accessed: 15 March 2024).

Turner, A. (2024) 'Reddit User Base & Growth Statistics: How Many People Use Reddit?', *bankmycell*, 4 March 2024. [Online]. Available at: https://www.bankmycell.com/blog/number-of-reddit-users/ (Accessed: 14 March 2024).

US Department of State (1987) 'Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87', vol. 9627, August 1987. [Online]. Available at: https://jmw.typepad.com/files/state-department---a-report-on-active-measures-and-propaganda.pdf (Accessed: 8 June 2024).

Wagner, J. (2021) 'Oracle named a Leader in the 2021 Gartner® Magic Quadrant™ for B2B Marketing Automation Platforms', *Modern Marketing Blog*, 6 October 2021. [Online]. Available at: https://blogs.oracle.com/marketingcloud/post/oracle-named-leader-gartner-magic-quadrant-b2b-marketing-automation-platforms (Accessed: 11 November 2023).

Wardle, C., Derakhshan, H. (2017) *Information disorder: Toward an interdisciplinary framework for research and policymaking.* Vol. 27. Strasbourg: Council of Europe.

Weedon, J., Nuland, W., Stamos, A. (2017) 'Information operations and Facebook' *Facebook*, 27 April. [Online]. Available at: https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf (Accessed: 5 January 2024).

WordPress (no date). [Online]. Available at: https://wordpress.com/ (Accessed: 15 March 2024).

Zahn, M. (2022) 'A timeline of Elon Musk's tumultuous Twitter acquisition', *ABC News*, 11 November 2022. [Online]. Available at: https://abcnews.go.com/Business/timeline-elon-musks-tumultuous-twitter-acquisition-attempt/story?id=86611191 (Accessed: 5 February 2024).

Zannettou, S., Bradlyn, B., De Cristofaro, E., Kwak, H., Sirivianos, M., Stringini, G., Blackburn, J. (2018) 'What is Gab: A Bastion of Free Speech or an Alt-Right Echo Chamber', *WWW '18: Companion Proceedings of the The Web Conference 2018*, pp. 1007–1014; https://doi.org/10.1145/3184558.3191531.

Zhou, R., Khemmarat, S., Gao, L. (2010) 'The impact of YouTube recommendation system on video views', *IMC '10: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pp. 404–410; https://doi.org/10.1145/1879141.1879193.

Cybercriminals are Using Paid Ads to Get to Top Cloud Provider's Customers (2015) *Trend-Micro*, 1 May 2015. [Online]. Available at: https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/cybercriminals-using-paid-ads-top-cloud-providers-customers (Accessed: 15 March 2024).

Statista (no date a) *Digital Advertising – Worldwide*. [Online]. Available at: https://www.statista.com/outlook/dmo/digital-advertising/worldwide (Accessed: 14 March 2024).

DISARM Foundation (2024). [Online]. Available at: https://www.disarm.foundation/ (Accessed: 16 February 2024).

Disqus (no date). [Online]. Available at: https://disqus.com/ (Accessed: 15 March 2024).

Last Week Tonight with John Oliver (2017) *Sinclair Broadcast Group*, 3 July 2017. [Online]. Retrieved: 15 March 2024, from HBO: https://www.youtube.com/watch?v=GvtNyOzGogc.

Statista (no date b) *Number of monthly active Facebook users worldwide as of 3rd quarter 2023*. [Online]. Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (Accessed: 9 February 2024).

Operation INFEKTION (2024) *Wikipedia*, 14 March 2024. [Online]. Available at: https://en.wikipedia.org/wiki/Operation_INFEKTION (Accessed: 8 June 2024).

Tracking Disinformation and Conflict (no date) *Empirical Studies of Conflict*. [Online]. Available at: https://esoc.princeton.edu/projects/tracking-disinformation-and-conflict (Accessed: 15 March 2024).

Chapter 17

Legal Aspects of Hybrid Threats and Warfare

Katarzyna Zombory

Abstract

The chapter addresses the selected legal aspects of hybrid threats and warfare connected to certain branches of the international public and European Union (EU) law. The overarching objective of the chapter is to present a legal assessment of hybrid threats and delineate the scope of lawful countermeasures to respond to them, which is a prerequisite for swifter decision-making and enhancing the defensive capability of the EU. The author outlines the conceptual framework of hybrid warfare and hybrid threats, exemplified by the hybrid tactics used in the 2014 Russian invasion against Ukraine. The legal analysis of hybrid threats and warfare is carried out under rules governing the lawfulness of the resort to force (*jus ad bellum*), international law of armed conflicts (*jus in bello,* international humanitarian law), and human rights law. This analysis demonstrates that it is difficult to conclude whether the use of hybrid threats and warfare amounts to the use of force, and whether it triggers legal consequences attached to the existence of armed conflict, in terms of the right to self-defence and application of international humanitarian law, especially if a hybrid campaign does not involve the use of kinetic force. While balancing between war and peace, hybrid threats and warfare highlight how the traditional dichotomy underlying the law on the use of force works in favour of hybrid aggressors. Compared to the international legal framework, the EU's framework "theoretically" offers wider possibilities for a collective response to hybrid threats and campaigns compared with the North Atlantic Treaty Organization (NATO). This is because the EU framework enables invocation of the mutual solidarity clause (Article 222 Treaty on the Functioning of the EU) in situations that otherwise would not trigger a collective defence mechanism under Article 5 NATO Treaty.

Katarzyna Zombory (2024) 'Legal Aspects of Hybrid Threats and Warfare'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 755–800. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_17

Keywords: hybrid threats, hybrid warfare, information warfare, lawfare, collective defence

1. Introduction

War and warfare undoubtedly belong to the core domain of military alliances, such as the North Atlantic Treaty Organization (NATO) or the Rio Pact. The deteriorating global security environment prompted the European Union (EU), an economic "civilian power" rather than a military alliance, to increase its defence and military capacity, based on the concept of strategic autonomy, and to recently adopt its first quasi-military doctrine (the 2022 Strategic Compass for Security and Defence).[1] In its efforts for preventing and countering global security threats, the EU has increasingly focused on creating a coordinated response system for hybrid threats and hybrid campaigns, alone and in concert with the NATO. The growing concern about hybrid threats comes from the acknowledgement that both state and non-state actors are increasingly using hybrid tactics, including information manipulation, to interfere with democratic processes, which pose a growing security threat to the NATO and EU. Over the last decade, several EU Member States and the EU as a whole have been victims of multiple hybrid attacks, which warn how hybrid adversaries can identify and exploit existing vulnerabilities to achieve their strategic goals.

Russia's annexation of Crimea in 2014 and its recent armed aggression against Ukraine in February 2022 demonstrated that modern armed conflicts come with the highest level of military force combined with hybrid tactics and information manipulation.[2] As the NATO Secretary General Jens Stoltenberg puts it, the tactics used by hybrid adversaries are a dark reflection of the NATO's comprehensive approach, used to maintain peace and stability around the world.[3] This "dark reflection" denotes the emergence and proliferation of hybrid warfare – in which international law plays a crucial role as a strategic enabler and operating environment – primarily to gain advantage over law-abiding states. Hybrid warfare is a logical consequence of the rivalry between two visions of the international community and international legal order: the vision of the West, formulated under the influence of the United States, and the vision shared by Russia and China, which rejects the United States' global hegemony and demands a multipolar international community.[4] In the non-

1 Council of the European Union, *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*, Brussels, 21 March 2022, 7371/22.

2 Council of the European Union, *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns*, Brussels, 21 June 2022, 10016/22, para. 1.

3 NATO, 2015.

4 For a detailed analysis of the problem, see: Mik, 2022; Aukia and Kubica, 2023.

Western narrative, one manifestation of the United States' hegemonic position is the unilateral and abusive interpretation of the law on the use of force by the NATO coalition. Non-Western actors perceive the NATO's 1999 Kosovo intervention (Operation Allied Force) as a violation of international law that remains unsanctioned. From the Russian perspective, the NATO is an illegal aggressor that acts under the guise of peacekeeping and crisis regulation and resorts to hybrid warfare; the NATO's conduct justifies and validates Russian countermeasures using an equal form of hybrid warfare.[5] As Najžer puts it straightforwardly, hybrid warfare is a tool of revisionist powers who seek to challenge the dominant world order.[6] In other words, we are witnessing a remodelling of the world's geopolitical landscape shaped after the end of the Cold War, in the process of which the use of hybrid warfare and weaponisation of international law is intrinsic.

This chapter's research objective is presenting a legal assessment of certain legal aspects connected to hybrid threats and warfare under various branches of the international public law and EU law. While this is a highly demanding if not an impossible task, analysing the legal framework applicable to hybrid conflicts and identifying its legal gaps should contribute to increasing the overall legal preparedness and legal resilience against hybrid threats in the EU and its Member States, even if there are no clear-cut answers to all the legal ambiguities. Delineating the scope of lawful countermeasures to prevent and respond to hybrid threats is a prerequisite for swifter decision-making and enhancing the EU's defensive capability. In section 2 of the chapter, the author addresses the terminological and conceptual framework of hybrid warfare and hybrid threats. Section 3 focusses on a legal analysis of hybrid threats and warfare carried out with respect to the following branches of international law: international law governing the lawfulness of the resort to force (*jus ad bellum*), international law of armed conflicts (*jus in bello*, international humanitarian law [IHL]), and human rights law. Section 4 of the chapter is devoted to the EU's approach to dealing with hybrid threats.

A legal assessment of hybrid threats and warfare is not possible without exploring the traditional dichotomy between war and peace that underlies the international legal regime on the use of force and law of armed conflicts. The reality of contemporary conflicts, which come with a combination of sophisticated non-kinetic and kinetic attacks that cannot be easily classified as either war or peace, prompts a dilemma reminiscent of the Schrödinger's paradox. In Schrödinger's famous experiment, the scientist argued that under certain conditions, the object of his experiment (a cat) can be simultaneously considered alive and dead. This chapter highlights the challenges posed by the use of hybrid threats and warfare for traditional legal classification, implying the unambiguous existence or non-existence of armed

5 See: the Federation Council of the Federal Assembly of the Russian Federation, 2019; Kremlin, Moscow, 2014. The Russian perspective and legal narrative are explained by Morten M. Fogt; see: Fogt, 2020, pp. 35–38, 47–49.

6 Najžer, 2020, p. 4.

conflict. This, with certain irony, can translate this chapter's research objective into the question of whether hybrid campaigns can substitute for Schrödinger's cat.

2. Concept and Means of Hybrid Threats and Warfare

2.1. Meaning of Hybrid Threats and Warfare

Throughout the past two decades, a considerable volume of scholarly works related to hybrid war has been published, resulting in an (over)abundance of definitions and ideas on what hybrid warfare is and how to term it properly.[7] The concept of hybrid warfare lies at the intersection of different disciplines, such as law, military doctrine, international relations, and security studies, which have employed various terms to describe the same phenomenon, such as low-intensive asymmetric warfare, fourth- or fifth-generation warfare, full-spectrum warfare, ambiguous warfare, grey-zone warfare, or sub-threshold warfare.[8] Following the Russian annexation of Crimea in 2014, NATO's term of choice has been "hybrid warfare".[9] In turn, EU documents employ the terms "hybrid threats" and "hybrid campaigns", avoiding the association with war and warfare.[10] This can be explained by the fact that the term "warfare" implies violent military activities, dealing with which is central for NATO; however, such activities lie on the outer periphery of the EU's mandate, while the word "threat" also covers less-intensive and non-violent acts and forms of confrontation.[11] Although several authors distinguish between these terms based on the intensity of the conflict and level of aggression,[12] legal challenges posed by hybrid warfare and hybrid threats are the same regardless of the denomination used. Therefore, this chapter uses both terms.

While the terms of hybrid threat and warfare are non-legal, they permeate the contemporary legal debate on the use of force. The reason for this is, on the one hand, the crucial role of law as a weapon and operating environment and, on the other, the consequences of the legal classification of hybrid conflicts on the targeted state or states' choice of defensive measures. Inherent to every legal debate is the attempt to define the notions under consideration and delineate their content. This seemingly basic task is not without significant difficulties in case of this chapter's

7 Besides numerous scientific articles, there have been several book-long accounts on hybrid warfare, e.g. Lasconjarias and Larsen, 2015; Mansoor, 2012; Najžer, 2020.
8 Fogt, 2020, p. 30.
9 Ibid.
10 See, e.g. Council of the European Union, *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns*, Brussels, 21 June 2022, 10016/22.
11 Dinstein, 2011, pp. 9–10; Sari, 2017, p. 15.
12 See e.g. Lott, 2022, pp. 16–17; Sari, 2017, p. 15.

topic. This is because there is no common understanding of what hybrid warfare is, let alone a universally accepted definition. Nevertheless, legal considerations of hybrid threats and warfare must be anchored in a certain theoretical background.

It is believed that the first definition of hybrid threats and warfare was coined by Frank Hoffman, a United States military writer, in the early 2000s. According to Hoffmann, 'hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder'.[13] Hoffman notes that hybrid wars are polymorphous in nature and can be conducted by both states and various non-state actors. He argues that the potential for types of conflict that blur the distinctions between war and peace and between combatants and non-combatants is on the rise.[14] Hoffman's understanding of a hybrid war is highly reminiscent of the concept of political warfare already used by American diplomat George F. Kennan in the 1940s to describe the nature of the Soviet threat. According to Kennan,

> … political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP), and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.[15]

Over the years, the conceptual idea of hybrid warfare has evolved, and many further definitions were proposed.[16] However, one aspect has been recurrent: A combination of various measures at the strategical, operational, and tactical level, with the goal of achieving strategical, political, and/or military advantages against another state, is inherent to the hybrid construct. The wide spectrum of means, both lawful and unlawful, including the legal framework and propaganda, effectively allow for the covered actions.[17] These elements permeate the NATO's discourse, where hybrid warfare is understood as a broad, complex, and adaptive combination of conventional and non-conventional means, as well as overt and covert military, paramilitary, and civilian measures, which are employed in a highly integrated design by state and non-state actors to achieve their objectives.[18] The EU, acknowledging that the definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, also construes the concept as a mixture of not only

13 Hoffman, 2007, p. 29.
14 Ibid., p. 7.
15 Kennan, 1948, para. 1.
16 Twenty years of the development and evolution of the hybrid warfare concept are captured by Johnson, 2021, pp. 45–57; Bekić, 2022, pp. 142–151.
17 Fogt, 2020, pp. 30–31.
18 NATO, 2016, para. 72.

coercive and subversive activity but also conventional and unconventional methods (i.e. diplomatic, military, economic, and technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.[19]

The NATO's recognition of the evolving character of 21st-century warfare and its endorsement of the comprehensive military approach[20] has met with firm doctrinal response from non-Western powers. The Russian apprehension of hybrid warfare, often referred to as the Gerasimov doctrine after the Chief of General Staff of the Armed Forces of Russia, recognises the nature of NATO's involvement in the Arab Spring as hybrid operations. Russian military leadership, following the coloured revolutions in Africa and the Middle East, declared that the rules of war had changed because the role of non-military means of achieving political and strategic goals had grown to exceed the power of force of weapons in their effectiveness. According to Gerasimov, the applied methods of conflict have changed in the direction of broad use of political, economic, informational, humanitarian, and other nonmilitary measures, applied in coordination with the protest potential of the population. Such methods are supplemented by military means of a concealed character, such as actions involving informational conflict and special-operations forces.[21] As Bekić notes, by reversing the NATO's comprehensive military approach (Stoltenberg's "dark reflection"), the Gerasimov doctrine has set the stage for Russian hybrid countermeasures, as they featured prominently in the subsequent conflicts in Ukraine.[22]

The recent Chinese military doctrine focussing on aggressive influence operations can be seen as a response to the changing nature of contemporary conflicts; it is also reminiscent of the ancient Chinese military strategy that saw subduing the enemy without fighting and using stratagems for deceiving and outwitting the enemy as the supreme art of war.[23] The United States' military involvement in the First Gulf War, Balkan wars, and 2003 invasion of Iraq have lead Chinese military strategists to realise that non-military operations and non-kinetic capabilities are central to fighting and winning contemporary conflicts.[24] China's strategic framework, adopted in 2003 and known as the "three warfares" strategy, encompasses three interrelated elements – psychological, public opinion (media), and legal warfare – indicating

19 European Commission, *Joint Framework on countering hybrid threats. A European Union response*, Brussels, 6.4.2016 JOIN(2016) 18 final, p. 2.

20 The NATO's comprehensive military doctrine implies engagement in six main domains: political, military, economic, social, infrastructure, and information. See: the NATO's contribution to a comprehensive approach in NATO, 2013, Chapter 1, points 1–2.

21 The English translation of Valery Gerasimov's paper 'Tsennost' nauki v predvidenii', originally published in *Voenno-promyshlennyi kur'er* in February 2013, is provided by Fogt, 2020, pp. 35–36. See also Johnson, 2015.

22 Bekić, 2022, p. 147.

23 According to Sun Tzu, 2010, Chapter V. III., point 2, 'Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting' (translated by Lionel Giles).

24 Clarke, 2019, pp. 189–191.

a comprehensive approach to waging conflicts.[25] The three warfares are complementary and mutually reinforcing, and they are considered a force multiplier in military operations and political or diplomatic scenarios.[26] The purpose of the three warfares is to establish "discursive power," understood as the power to control perceptions and shape narratives that serve Chinese interests, while undermining those of an opponent.[27]

Among Western scholars, two main approaches or schools of thought have developed as regards the conceptual framework of the hybrid threat and warfare. The first school assumes that hybrid warfare is not a new concept, as the combination of different means of waging war using regular and irregular forces has been known since ancient times. The second school of thought believes that hybrid warfare is a novelty that prompts the need to develop entirely new responses to it. According to this approach, hybrid threats and warfare are more than a combination of different modes of waging war or simultaneous use of regular and irregular forces. The novelty lies in modern actors' blending of conventional and conventional means in a way that enables them to remain in the so called "grey zone" between war and peace and to achieve their goals without crossing the threshold of war, through their ability to plausibly deny any involvement in hostile activities.[28] The abundant range of innovative technologies available in the 21st century, as well as the resourcefulness of hybrid adversaries, undoubtfully amounts to another significant *novum* of hybrid warfare. Nevertheless, from a legal perspective, this debate is of more academic than practical significance.

Although there is no universally agreed definition of hybrid threats and warfare, certain common characteristics can be identified to describe hybrid activities and facilitate their early detection. Distinguishing features relate to both means employed by hybrid adversaries and the destructive results of concerted hybrid attacks.

2.2. Examples of Hybrid Threats and Warfare

A hybrid arsenal encompasses an extensive array of lawful and unlawful means; any actions designed to destabilise a given society can be used within a hybrid campaign.[29] Hybrid threats and warfare may consist of political activities; (dis)informational campaigns; and cyber, military, economic, and societal interventions. The toolbox of hybrid threats and warfare includes, without being exhaustive, cyberattacks, terrorism, organised crime, application of covert psychological operations, drug trafficking, inducing of migration flows, espionage, infiltration, kidnapping,

25 Martin, 2021.
26 Kania, 2016.
27 Cochran, 2020, pp. 3–4.
28 Bekić, 2022, p. 148; Fogt, 2020, pp. 33–34; see also Johnson, 2021, p. 47.
29 Parulski, 2016, pp. 11–12; Sanz Cabellero, 2023, p. 2. Measures undertaken by hybrid adversaries target the full spectrum of the society, affecting the given state's apparatus and population as a whole; hence, information influence plays a crucial role in hybrid conflicts.

economic leverage, media exploitation, use of unmarked special forces, mercenaries or proxy soldiers, intimidation and propaganda, or instrumental and abusive use of the legal framework.[30]

Fogt describes hybrid threats and warfare as a mixture of hybrid orchestrated non-kinetic and kinetic efforts, which may be based on, among others, (1) organised and controlled actions at the highest political and military levels supporting a clear long-term strategic vision; (2) unclear distinction between peace, crisis, and war and thus operations in various legal grey zones; (3) hybrid hostile engagement in terms of full-spectrum actions, including cyberspace and information activities; (4) strategy of denial regarding overall or effective control over non-state actors and motivation of civilians to participate in propaganda and cyberattacks; (5) protection and shielding of non-state actors and civilians participating in unlawful hybrid activities from national and international prosecution; (6) use of publicly controlled or influenced media and the private economic sector; (7) use of trade and economic state sanctions, that is, export or import restrictions, under the pretext of political and legal justification; (8) targeting of specific vulnerabilities of all possible counterparties, including defence alliances, individual states, international organisations, non-state actors, and foreign populations; (9) exploitation of existing weaknesses – such as lack of consensus in democracies and alliances, absence of political willingness to react, and reduced capacities to act with a timely response – and thus a reliance on late reaction instead of prompt action by opponents; and (10) use of "lawfare" for promoting one's own actions as legitimate and opponents' reactions as unlawful.[31]

Bachmann and Munoz Mosquera argue that hybrid adversaries resort to means based on indirect and multidisciplinary approaches (civil and military, legal and illegal, kinetic and non-kinetic, high-tech, etc.) to erode and delegitimise the internal and external prestige, reputation, and support of a superior military force, state apparatus, and/or international organisation; create confusion in general by questioning agreed political, religious, or territorial status quo; and build new dependencies and structures based on essential resources to support consolidated or imposed political, religious, or territorial changes.[32]

A distinctive feature of hybrid threats and warfare is the legal imbalance between law-abiding democratic states and illegally acting autocratic states or non-state actors.[33] Hybrid adversaries can attain legal asymmetry, which considerably limits

30 The NATO Strategic Communications Centre of Excellence provides for a systematised overview of hybrid threats and warfare identified in 30 case studies, by grouping them into the categories of diplomatic, information, military, economic, financial, intelligence, legal, and law enforcement measures; Heap, 2021, pp. 30–36. Another informative list of tools of hybrid threat activities is included in the joint report of the European Commission and Hybrid CoE on a conceptual model of hybrid threats; Giannopoulos, Smith and Theocharidou, 2021, pp. 33–35.

31 Fogt, 2020, p. 33.

32 Munoz Mosquera and Bachmann, 2016, p. 68.

33 For example, Fogt, 2020, p. 32; Sari, 2017, p. 26.

the countermeasures and defensive powers available to targeted states, through the instrumental use (weaponisation) of law, often referred to as lawfare and the exploitation of legal grey zones. The term "lawfare" denotes a method of warfare wherein law is used as a means of realising a military objective; in other words, it is the use of law as a weapon of war or, to quote Charles J. Dunlap, 'a cynical manipulation of the rule of law and the humanitarian values it represents'.[34] Instrumentalisation of law has the goal of manipulating the law by changing legal paradigms; creating confusion about the source of applicable law; and hampering consequent actions to identify the perpetrator, assign legal responsibility, and demand accountability.[35] Sari argues that hybrid adversaries aim to create legal asymmetry by (1) exploiting legal thresholds, complexity, and uncertainty; (2) generating legal ambiguity; (3) violating their legal obligations; and (4) utilising law and the legal process to create narratives and counter-narratives.[36]

Another distinctive tool of hybrid hostilities that commonly features in contemporary hybrid conflicts is information operations and influence activities, the conduct of which can be loosely termed as "information warfare". There is no clear definition or conceptual framework on information warfare. In general terms, it can be seen as a struggle to control or deny the confidentiality, integrity, and availability of information in all its forms, ranging from raw data to complex concepts and ideas.[37] Offensively, information warfare occurs when one side of a conflict seeks to impose its desired information state on the adversary's information and affect how target individuals or populations interpret or learn from the information they possess or collect. Defensive information warfare occurs when one side seeks to retain the ability to freely collect, interpret, and/or learn from its available information without outside interference.[38] Information warfare combines electronic warfare (including electronic countermeasures and jamming), cyberwarfare, and psychological operations, aimed at degrading the morale and well-being of a nation's citizens, such as by spreading false information through social media and news outlets.[39] Consequently, two main types of hybrid attacks with relation to the information environment can be identified: (1) attacks related to (dis)information that aim to provoke decision-making errors and (2) attacks that directly affect physical systems.[40] Countering information warfare and influence operations is particularly challenging due to the international human rights framework, which provides for wide guarantees of the right to freedom of expression. Determining what content falls within the ambit of freedom of expression and what qualifies as foreign interference is crucial, although

34 Dunlap, 2021, p. 4. For more accounts of lawfare, see: Dunlap, 2008; Kittrie, 2016; Kowalczewska, 2014; Munoz Mosquera and Bachmann, 2016; Veress, 2023.
35 Munoz Mosquera and Bachmann, 2015, pp. 26–27.
36 Sari, 2017, pp. 28–30.
37 Bingle, 2023.
38 Ibid.
39 Committee on Legal Affairs and Human Rights, 2018, p. 7.
40 Medina Llinàs, 2022, p. 39.

far from obvious. The example of Russian "troll factories" (or "troll farms") illustrates the challenges related to distinguishing the line between state interference and online activists' right to freedom of expression, and it highlights the scale of threat posed by information operations.[41]

Information warfare holds a paramount place in the military strategy and international relations of non-Western powers, such as Russia and China. It permeates the military doctrine of the Russian Federation, where it is associated with the "reflexive control theory" and constitutes a vital component of Russia's contemporary hybrid warfare strategy.[42] The aim of reflexive control actions is to influence the adversary's political or military plans, understanding of the situation, and decision-making processes, thereby taking control over their decisions and pushing them to make unfavourable political or military choices.[43] The major part of Russian reflexive control-based hybrid threat efforts are aimed at dividing Western allies and altering their collective decision-making processes.[44]

Recent frontier incidents in several EU Member States involving state-sponsored, artificially induced mass movement of irregular migrants provide further examples of hybrid tactics. The weaponisation of migrants, also termed "coercive engineered migrations", has been employed, such as on the Greece-Turkey border (2020) and the Lithuania-Belarus, Latvia-Belarus, and Poland-Belarus borders (2021), as a tool to compel the EU to make political and financial concessions, or in the case of the 2021 frontier incidents, to coerce the EU to withdraw its support for democratic movement in Belarus. The 2020 and 2021 border incidents exploited internal division among EU Member States on the issue of illegal migration, a vulnerability that became evident during the 2015 migration crisis.[45] The Prime Ministers of Poland, Lithuania, Latvia, and Estonia;[46] President of the European Commission Ursula von den Leyen; and President of the European Council Charles Michel explicitly labelled these hybrid operations as hybrid attacks to destabilise Europe.[47] In response to the 2021 hybrid attacks, the EU amended its sanctions regime to be able to respond to the instrumentalisation of migrants for political purposes and subsequently adopted restrictive measures (sanctions) on Belarus.[48]

41 Russian interference in the 2016 United States presidential elections has been alleged to involve Russian troll farms using divisive topics such as gun control and racial conflict to polarise voters and plant disinformation; Yablokov, 2022, p. 767.

42 Franke, 2015, pp. 11–12. While confusing the enemy and distorting the perception of real facts are key tactics of Russia's information war concept, reflexive control provides a theoretical foundation and tools for achieving it; Aukia and Kubica, 2023, pp. 34–35.

43 Aukia and Kubica, 2023, p. 35.

44 Ibid.

45 For the artificially engineered migration crisis, see: Bekić, 2022; Greenhill, 2010; Łubiński, 2021; Sari, 2023.

46 *Statement of the Prime Ministers of Poland, Lithuania, Latvia and Estonia on the hybrid attack on our borders by Belarus*, 2021.

47 European Commission, 2021a; European Commission, 2021b; European Council, 2021.

48 Council of the EU, 2021a; Council of the EU, 2021b.

The Russian Federation's 2014 intervention in Crimea is considered an archetypal example of a hybrid conflict.[49] The Russian campaign was carried out with a combination of various kinetic and non-kinetic means, which involved, among others, using proxy soldiers and unmarked special forces ("little green men"), provoking internal disturbances, conducting information operations, and making instrumental (mis)use of the international legal framework on the protection of national minorities and prevention of genocide.[50]

A cybercampaign to blur factual reporting and manipulate public opinion played a prominent role in the Russian hybrid arsenal used against Ukraine in 2014. Aside from social engineering and information warfare-style attacks, malicious software was installed in Ukrainian government and military artillery systems, while botnet attacks targeted Ukrainian websites and Ukrainian electoral systems.[51] An eye-opening research by John E. Arthur VI on the Russian cybernetwork operations in Estonia (2007), Georgia (2008), and Ukraine (2014) shows that Russia has long been using cyber and influence operations to support its military operations in the central regions of the former Soviet Bloc. Arthur demonstrates that a clear pattern can be identified in the Russian cybernetwork operations, which consist of three deliberate phases of cyber-support to potential Russian military operations, two of which include extensive inform-and-influence activities.[52]

The 2014 hybrid campaign involved large-scale use of legal arguments to support violent operations and other hybrid actions. Examples of how the Russian Federation used lawfare in the 2014 hybrid operation against Ukraine are plentiful: amending domestic laws on incorporation of territories into the Russian Federation, allowing the annexation of parts of neighbouring states following popular local referenda (in February–March 2014), modifying the law applicable to citizenship and using residency claims dating back to the Soviet Union and Russian Empire to grant Russian citizenship (April 2014); issuing Russian passports to claim the presence of Russian citizens in neighbouring regions (Abkhazia, South Ossetia, and Crimea);

49 Heap, 2021, p. 12. Although Russia had used a combination of military and non-military tactics in Georgia in 2008, they were only described as "hybrid" retrospectively.

50 Heap, 2021, p. 12; Parulski, 2016, pp. 12–15; Veress, 2023, pp. 35–36.

51 The sequence of Russian cybercampaigns' targets in 2014 was as follows: (1) Ukrainian populace, (2) governmental systems, (3) military systems, (4) Ukrainian websites, (5) Ukrainian electoral systems, and (6) Ukrainian utility systems; Arthur, 2020, pp. 51–52.

52 The first phase of Russian cybercampaigns tends to be a shaping operation, which creates conditions for the success of the decisive operation or kinetic attack; it targets, via malware, governmental and military organisations. The second phase is a sustaining operation, which focuses on information technology, media, and news targets and coincides with social media disinformation campaigns designed to dominate the information spectrum and create confusion. The final phase, disruption, focusses on dominating the adversary via inform-and-influence activities and computer network attacks. These attacks tend to consist of distributed denial-of-service/Structured Query Language injection-type attacks aimed at governmental and military targets; information technology, media, and news targets; and financial and business institutions. By attacking and disrupting such targets, Russia can effectively distract the targeted citizens from rapidly developing into an insurgency or organising a more robust means of defence; Arthur, 2020, pp. 52–53.

making attempts to use the United Nations (UN) Security Council to sanction the potential Russian opening of humanitarian corridors, using Kosovo and Libya as legal precedents for Russian actions; Russian courts sentencing Ukrainian officials *in absentia*; and Russian propaganda fabricating a legal case to justify the deployment of Russian "peacekeeping forces" in East Ukraine to prevent "a humanitarian catastrophe" caused by the "genocide" of Russian speakers in the region (examples from Voyger).[53]

Aside from the above-mentioned examples of instrumentalisation of law, the different narratives on the 1994 Budapest Memorandum on Security Assurances,[54] signed by the United States, Russia, Ukraine, and the United Kingdom in connection with Ukraine's accession to the 1968 Treaty on the Non-Proliferation of Nuclear Weapons,[55] show how the interpretation of international obligations can be used as lawfare. Signatories of the Budapest Memorandum pledged to respect the independence, sovereignty, and existing borders of Ukraine and to refrain from the threat or use of force against the territorial integrity or political independence of Ukraine, undertaking that none of their weapons will ever be used against Ukraine except in self-defence or otherwise in accordance with the UN Charter.[56] Russia breached these commitments by the annexation of Crimea in 2014 and subsequent aggression in Ukraine; however, Russian officials asserted that the loss of Ukraine's territorial integrity has resulted from complicated internal processes, which Russia and its obligations under the Budapest Memorandum have nothing to do with.[57] Such deliberate misinformation about the scope of treaty obligations and the attempt to negate the validity of an international treaty, which runs afoul of the principle *pacta sunt servanda*, demonstrates the lack of good faith and amounts to a case of treaty abuse, potentially giving rise to state responsibility.[58] Mosquera and Bachmann note that by distorting international law, Russia has engaged in hybrid warfare against not only Ukraine but also the entire NATO.[59] In this context, it is important to note that the 1994 Budapest Memorandum was purposefully designed to be ambiguous to allow its signatories to achieve significant goals. It provides a clear example of how legal ambiguities can become vulnerabilities that are exploited by hybrid adversaries.[60]

53 Voyger, 2015, p. 20.

54 *Memorandum on security assurances in connection with Ukraine's accession to the Treaty on the Non-Proliferation of Nuclear Weapons*, signed in Budapest on 5 December 1994, UN Treaty Series vol. 3007, No. 52241.

55 *Treaty on the Non-Proliferation of Nuclear Weapons*, concluded in Washington, Moscow, London on 1 July 1968, UN Treaty Series vol. 729, No. 10485.

56 Articles 1 and 2 of the Budapest Memorandum.

57 Statement of the Russian Minister of the Foreign Affairs, Alexander Lukashevich, of 12 March 2015, cited in Munoz Mosquera and Bachmann, 2015, p. 27.

58 Munoz Mosquera and Bachmann, 2015, p. 27.

59 Munoz Mosquera and Bachmann, 2016, p. 84.

60 For a detailed analysis of the 1994 Budapest Memorandum in the context of the Russia-Ukraine war, see Soldatenko, 2023.

The 2014 Russian hybrid attacks against Ukraine, the intensity of which reached its peak with the annexation of Crimea in February–March 2014, amounted to acts of aggression contrary to the prohibition of the use of force set forth in the UN Charter.[61] Although, in February 2022, the initial hybrid conflict transformed into a conventional high-intensity military conflict, this full-scale military conflict has constantly been a theatre of various hybrid operations, including, but not limited to, actions aimed at triggering energy, humanitarian, and food crises. The commercial blockade of Black Sea ports is an illustrative example of hybrid tactics used in the 2022 Russian military invasion against Ukraine. The blockade resulted in a disruption of Ukrainian grain exports. However, seen from a wider perspective, this not only deprived Ukraine of its key revenue source but also aimed to cause a food crisis at the regional and global levels. This further destabilised the situation in Africa and the Middle East and hobbled the already critical global security situation.[62] Overall, through its hybrid actions in 2022 and 2023, Russia aimed to reduce Western support for Ukraine and weaken the cohesion of NATO and the EU.[63]

3. Legal Assessment Under Public International Law

Hybrid threats and warfare can be examined from different angles with respect to different fields of public international law. First, hybrid threats and warfare are examined in the context of international law on the use of force (*jus ad bellum*) through the prism of prohibition on the use of force and the exceptions thereto, such as the right to individual and collective self-defence, and in the context of attribution of responsibility. The aim is to answer the following: (1) Can the use of hybrid threats and warfare trigger the right to individual or collective self-defence? (2) If military countermeasures are not a lawful response to hybrid activities, what defence measures can be lawfully implemented against aggression below the threshold of an armed attack? (3) Can hybrid adversaries face the responsibility for international wrongful acts on account of the use of hybrid threats and warfare? Second, hybrid activities are assessed from the perspective of IHL (*jus in bello,* law of armed conflicts), in terms of both international and non-international armed conflicts. Finally, hybrid threats and warfare are examined from the perspective of international human rights law to determine whether, and to what extent, countering hybrid threats can entail the curtailment of fundamental rights and freedoms.

61 *Charter of the United Nations*, adopted in San Francisco on 26 June 1945, XV UNCIO 335. See, e.g. European Council, 2014, para. 2; Wyrozumska, 2014, pp. 277–278.
62 Ionita, 2023.
63 Ibid.

3.1. Jus ad bellum

The international law governing the use of force rests upon the general prohibition of the threat or use of force between states, as expressed in Article 2 para. 4 UN Charter, which states that 'All Members shall refrain in their international relations from *the threat or use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations' (emphasis added). The ban on the unilateral use of force is a universally accepted norm of customary international law.[64] It constitutes one of the core values of the international community as a principal element of the international system of war prevention. In the UN Charter, the general prohibition of force is subject to two exceptions. They encompass, first, collective actions of the UN Security Council to maintain or restore international peace and security, implemented under Chapter VII of the UN Charter. Until the Security Council has taken collective actions, the state or states under attack can resort to individual or collective self-defence, which accounts for the second exception to the ban on the recourse to inter-state military action. Defensive use of force is permitted under Article 51 UN Charter, which states that the UN Charter does not impair 'the inherent right of individual or collective self-defence if *an armed attack* occurs against a Member of the United Nations' (emphasis added). The use of force in response to an armed attack is subject to the principles of proportionality, necessity, and immediacy, which aim to avoid escalation of conflicts through strict requirements for a permissive collective armed response.[65] The principle of self-defence, outlined in Article 51 UN Charter, provides a legal anchor for the collective defence mechanism enshrined in Article 5 of the NATO's founding treaty – the North Atlantic Treaty (hereinafter, the NATO Treaty)[66] – the cornerstone of the NATO Alliance, as well as in several regional collective defence mechanisms, such as those existing under the EU framework (mutual

64 Dörr and Randelzhofer, 2015, p. 203. The first international treaty on the renunciation of war as an instrument of international relations was adopted in 1928 (Briand-Kellog Pact), with which international law moved from *jus ad bellum* to *jus contra bellum*. For the historical development of the ban on the use of force, see, e.g. Dinstein, 2011, pp. 81–88; Dörr and Randelzhofer, 2015, pp. 204–207.

65 Fogt, 2020, pp. 69–70. For related case law of the International Court of Justice (ICJ), see, e.g. ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*, Merits, judgement of 27 June 1986, https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf; ICJ, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, judgement of 6 November 2003, https://www.icj-cij.org/sites/default/files/case-related/90/090-20031106-JUD-01-00-EN.pdf; ICJ, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Rwanda)*, judgement of 19 December 2005, https://www.icj-cij.org/sites/default/files/case-related/116/116-20051219-JUD-01-00-EN.pdf.

66 *North Atlantic Treaty*, signed in Washington on 4 April 1949, UN Treaty Series vol. 34, Registration No. 541.

defence clause in Article 42 para. 7 of the Treaty on the EU) or within the Organization of American States (Article 3 para. 1 of the Inter-American Treaty of Reciprocal Assistance).[67]

According to the prevailing interpretation of Article 2 para. 4 UN Charter, prohibition of the 'threat and use of force' covers only the use of armed force, that is, military force, and it does not extend to "any" possible use of force.[68] Consequently, psychological or economic pressure, which often forms part of the hybrid arsenal, does not amount to the use of force within the meaning of Article 2 para. 4 UN Charter, unless combined with the use of armed forces.[69] Therefore, it can be established that targeting a state or states with hybrid threats and warfare, which do not involve violent acts, will not be considered waging "war" in the meaning of illegal use of force under Article 2 para. 4 UN Charter.[70] Neither does it qualify as "aggression" in terms of the UN General Assembly Resolution 3314 (XXIX) on the definition of aggression.[71] The 2014 Russian hostilities against Ukraine were considered acts of direct aggression in violation of the prohibition of threat or use of force, primarily because of the deployment of Russian armed forces in Ukraine and illegal acquisition of part of its territory, and not as a direct consequence of disinformation campaigns, cyberattacks, or weaponisation of law, also widely employed by Russia during the 2014 hybrid conflict.

The inherent right to self-defence under Article 51 UN Charter is not linked to the illegal "use of force" but is dependent on the existence of an "armed attack". The threshold for an armed attack is considered higher than that for the use of force, implying that all armed attacks classify as the use of force, but not every use of force qualifies as an armed attack.[72] According to the International Court of Justice (ICJ), the essential criteria that need to be considered when assessing whether hostilities level up to armed attack are their scale and effects.[73] Nonetheless, the relevant provisions of the UN Charter do not establish any gravity requirement, nor is the existence of the *de minimis* threshold for an armed attack undisputed in the international legal doctrine.[74] From the perspective of hybrid threats and warfare, the gap between the

67 *The Inter-American Treaty of Reciprocal Assistance*, signed in Rio de Janeiro on 2 September 1947, Organization of the American States Treaty Series Nos. 8 and 61 (also called the Rio Pact).

68 Dörr and Randelzhofer, 2015, pp. 208–209.

69 Dinstein, 2011, p. 88; Dörr and Randelzhofer, 2015, pp. 208–210. Nevertheless, such conduct may amount to a breach of the principle of non-interference in domestic affairs.

70 Instead of condemning the "resort to war", drafters of the UN Charter rephrased the term used in Article I of the 1928 Briand-Kellog Pact to 'threat or use of force'. The goal was to settle the discussion on the scope of the prohibition of war by prohibiting the deliberate initiation of force, whether or not the hostilities amounted to the normative condition of "war"; see: Lauterpacht, 1968, p. 62; Lesaffer, 2015, p. 54.

71 General Assembly Resolution 3314 (XXIX) Definition of Aggression, 14 December 1974, A/RES/3314(XXIX).

72 As recognised by the ICJ in *Nicaragua v. United States of America*, paras. 191–195; see also Dinstein, 2011, pp. 207–210; Hathaway, 2014, p. 214; Schmidt, 2015, p. 1119.

73 ICJ, *Nicaragua v. United States of America*, para. 195.

74 Fogt, 2020, pp. 63–64; Sari, 2017, pp. 23–24.

use of force and armed attack represents a serious obstacle for legal inter-operability, meaning there are difficulties related to the legal assessment of the situation and available countermeasures. In parallel, the gap between Article 2 para. 4 and Article 51 UN Charter creates an important advantage for hybrid adversaries by setting the stage for conducting hostilities at such a level of intensity or in a form that does not invest the targeted state with the right to use force in self-defence (as long as it is kept below the threshold for an armed attack).[75]

There have been several attempts at clearing the legal fog of hybrid war. Fogt suggests that in the face of low-intensity hybrid threats designed to remain below the threshold of an armed attack, the theory of "accumulation of events" can provide a useful tool to facilitate the threats' legal assessment. The asymmetric hybrid character of low-level use of force, flexibility in the intensity, and disinformation and fake news campaigns targeted at the entire papulation may collectively level up to an "armed attack".[76] The possibility of cumulatively weighting a series of acts to categorise them as an armed attack that justifies the right to use self-defence has been established by the ICJ[77] and has received support in the international legal doctrine.[78] In other words, the theory of accumulation of events provides the targeted state or states a legal possibility to exercise the right of self-defence in case of a hybrid campaign that otherwise is designed to remain below the threshold of an armed attack. Nevertheless, even if the accumulation of several low-intensity hybrid hostilities can be classified as an armed attack within the meaning of Article 51 UN Charter, it must be demonstrated that the hybrid hostilities originate from a specific state or non-state actor, and that they are attributable to those states or non-state actors, which, as the practice shows, is difficult due to the use of proxy actors, proxy networks, or a denial policy.

According to Dörr and Randelzhofer, the weapon-like destructive potential some attacks might develop using information technology legitimises an exception to the narrow interpretation of the term "force" in Article 2 para. 4 UN Charter as solely military force.[79] In extreme situations, computer network attacks against the information systems of another state might produce the effects of an armed attack triggering the right to self-defence under Article 51 UN Charter and allow the targeted state to respond by using armed force without violating Article 2 para. 4 UN Charter.

75 Sari, 2017, p. 23. There are several further legal issues connected to the use of force in legitimate self-defence that belong to complex legal grey zones: quality and quantity of the target of an armed attack (territory, infrastructure, military facilities, population, and person), burden of proof, and need of a possible intention; Fogt, 2020, p. 66.

76 Fogt, 2020, pp. 66–67.

77 *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*), para. 64. The ICJ examined the hostile incidents cumulatively to consider that they did not constitute an armed attack on the United States of the kind that, in line with the test used in the Nicaragua case, could have been qualified as a "most grave" form of the use of force, justifying the right to self-defence under Article 51 UN Charter.

78 Dinstein, 2011, pp. 206–207.

79 Dörr and Randelzhofer, 2015, p. 210; similarly, Dinstein, 2011, p. 212.

A similar approach is adopted by Dinstein, according to whom the main consideration while assessing weapons for the purpose of an "armed attack" within the meaning of Article 51 UN Charter is their consequential effects.[80] Thomas P. Jordan suggests that to determine whether a cyberattack constitutes an act of war, the ends sought from the attack should be examined. There is a substantial difference between a cyberattack to steal sensitive documents and a cyberattack to disable the targeted state's ability to control its nuclear arsenal or central weapons system – only the latter is an act of war, while the former is merely an act of espionage.[81] In light of these considerations, it can be argued that if a hybrid campaign involving, *inter alia*, a computer network attack was to cause severe damage to property or even human fatalities, or seriously affect the targeted state's defensive capacities, it could be qualified as an armed attack, thus investing the affected state with the right to defensive use of force.

The 2014 Russian operations in Ukraine have prompted the necessity to evaluate the right to collective self-defence in the event of a hybrid threat or warfare. In 2015, NATO Secretary General Jens Stoltenberg publicly declared that the Alliance and its allies are prepared to counter hybrid warfare as part of collective defence under Article 5 NATO Treaty.[82] The 2022 NATO Strategic Concept endorsed Stoltenberg's earlier declaration and confirmed that the hybrid operations against Allies could reach the level of an armed attack, which can eventually lead the North Atlantic Council to invoke Article 5 NATO Treaty.[83]

Nevertheless, a key feature of most hybrid threats and warfare is that they operate below the threshold of armed conflict and therefore do not allow for the activation of individual or collective self-defence within the meaning Article 51 UN Charter, Article 5 NATO Treaty, or other defence alliance treaties. Therefore, the lawful answer to hybrid threats or warfare is, in most cases, limited to peacetime cooperation and non-forcible countermeasures. At the domestic level, the victim state can answer to hybrid threats short of an armed attack by implementing measures belonging to the peacetime and crisis (public emergency) legal framework. If a hybrid threat merely constitutes a breach of the principle of non-intervention, which does not level up to

80 Dinstein, 2011, p. 212.

81 Jordan, 2016, pp. 56–57.

82 Warsaw Summit Communiqué; see: NATO, 2016. Pursuant to Article 5 NATO Treaty,

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

83 A similar conclusion has been drawn with respect to malicious cyber-activities; see: NATO, 2022, paras. 25, 27.

an armed attack, it is still possible for the affected state to employ peaceful countermeasures, such as retaliatory measures through retorsions.[84] A more coordinated response is available under Article 4 NATO Treaty, which provides for a joint consultation forum for the Allies: 'The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened'.

The attribution of responsibility for hybrid operations to a particular state or non-state actor is a major difficulty, considering that states often use proxies to operate in the grey zone and avoid accountability. The state denial policy and covert operations by proxies and provocateurs, such as private military contractors and non-uniformed special forces, is central to hybrid warfare.[85] Moreover, global cyber-networks that hybrid adversaries commonly use allow different actors to commit acts of hostility while disguising their location or involvement. Even if the location from where a cyberattack was initiated can be identified, determining whether the attack was state-sponsored or whether the attackers operated under the protection of the state might still be an arduous task.

Holding a hybrid aggressor accountable requires establishing who had control over a given hybrid operation or who sponsored it.[86] If the given hybrid operation can be tracked back and attributed to a particular state actor, the rules of state responsibility codified in the draft Articles on the Responsibility of States for Internationally Wrongful Acts[87] are applicable. They establish two conditions for an action or omission of a state to be considered an internationally wrongful act: (1) The conduct of the state must be attributable to the state under international law, and (2) with such conduct, the state must have breached its international obligation.[88] They also provide for a set of rules governing the attribution of the actions and omissions to the state. Besides the clear-cut case wherein the actions or omissions of the state organs account for the conduct of the state, the conduct of a person or entity that is not a state organ, but is empowered by the state's law to exercise elements of governmental authority, can also lead to the attribution of wrongful conduct to the state if it acts in that capacity in the particular instance, even if it exceeds its authority or contravenes instructions.[89] What is important from the perspective of hybrid conflicts in which the use of proxies is commonplace is that the conduct of a person or group of persons is considered an act of a state under international law if that person or group of persons is in fact acting on the instructions of, or under the direction or

84 Karski and Mielniczek, 2019, p. 78.
85 Fogt, 2020, p. 74.
86 Sanz Cabellero, 2023, p. 6.
87 *Articles on Responsibility of States for Internationally Wrongful Acts*, UN General Assembly Resolution 56/83 of 12 December 2001, A/RES/56/83. Although the document has not been adopted as an international treaty, some of its contents reflect customary law; Sanz Cabellero, 2023, p. 6.
88 Article 2 of the Articles on Responsibility of States for Internationally Wrongful Acts.
89 Articles 4–5 and 7 of the Articles on Responsibility of States for Internationally Wrongful Acts.

control of, that state (i.e. conduct directed or controlled by the state).[90] A conduct not attributable to a state according to the previous rules will nevertheless be considered an act of that state under international law if the state acknowledges and adopts the conduct as its own.[91] Finally, several circumstances preclude the wrongfulness of conduct, such as when the act constitutes a lawful measure of self-defence taken in conformity with the UN Charter or is a countermeasure taken against another state in breach of its international obligations.[92]

By way of illustration, hostilities during the 2014 Russian-Ukrainian hybrid conflict that were performed by irregular forces (little green men) on the Crimean Peninsula can be attributed to the Russian Federation based on several provisions of the 2001 draft Articles on the Responsibility of States for Internationally Wrongful Acts. First, during an annual televised meeting with the Russian nation on 17 April 2014, President Putin (eventually) admitted that the "little green men" acting in Crimea were Russian servicemen.[93] This allowed a formal qualification of their activities as having been carried out by the Russian Federation itself based on Article 4 of the draft Articles. Second, in the light of President Putin's statement, the responsibility of the Russian Federation for the activity of irregular forces could also be based on Article 11 of the draft Articles, according to which the state bears international responsibility for an activity that it acknowledges and adopts as its own. These actions, attributed to the Russian Federation, constituted a breach of its international obligations, such as the obligation to refrain from the use of force against territorial integrity stemming from Article 2 Budapest Memorandum. Therefore, the conditions for considering that Russia committed an internationally wrongful act were formally met.

The 2001 draft Articles on the Responsibility of States for Internationally Wrongful Acts can provide an adequate framework to address state-sponsored hybrid threats and warfare. Nevertheless, they do not eliminate two main challenges relating to the attribution of responsibility for hybrid operations: hybrid threats that cannot be attributed

90 Article 8 of the Articles on Responsibility of States for Internationally Wrongful Acts.

91 Article 11 of the Articles on Responsibility of States for Internationally Wrongful Acts.

92 Articles 21–22 of the Articles on Responsibility of States for Internationally Wrongful Acts.

93 Earlier in 2014, President Putin denied on numerous occasions that the well-equipped troops operating in Crimea and wearing green uniforms without insignia had been part of the Russian armed forces. On 17 April 2014, President Putin, while opposing the use of the term "little green men," said, '… one cannot apply harsh epithets to the people who have made a substantial, if not the decisive, contribution to enabling the people of Crimea to express their will. They are our servicemen'. While answering the question of who were the little green men, President Putin replied,

… our goal was to ensure proper conditions for the people of Crimea to be able to freely express their will. And so we had to take the necessary measures in order to prevent the situation in Crimea unfolding the way it is now unfolding in southeastern Ukraine. We didn't want any tanks, any nationalist combat units or people with extreme views armed with automatic weapons. Of course, the Russian servicemen did back the Crimean self-defence forces. They acted in a civil but a decisive and professional manner ….

For the English transcript of the annual special Direct Line with Vladimir Putin of 17 April 2014, see President of Russia, 2014. For an account of Russia's use of unmarked special forces as a tool of the 2014 hybrid conflict in Ukraine, see: Wentzell, 2021.

to any state actor and difficulties related to identifying the hybrid aggressors before any attempts to establish the connection with any state actor. In the first case, when a non-state actor is identified as a hybrid aggressor, as a rule, the targeted state's domestic criminal law will apply in terms of the attribution of responsibility.[94] The latter problem justifies the need for novel approaches. For example, Thomas P. Jordan suggests regarding cyberattacks – a particularly challenging form of hybrid threats and warfare in terms of identifying the attackers – that governments from whose territories the cyberattacks are launched should be mandated to participate in identifying the attackers or face the presumption that the state itself was coordinating the attack.[95]

3.2. *Jus in bello*

The IHL (law of armed conflicts, *jus in bello*) is a body of international law that governs the conduct of hostilities during an armed conflict, to limit its effects for humanitarian reasons. *Jus ad bellum* is distinct from *jus in bello*, as the former's application is not contingent on the legality of the armed conflict; consequently, it applies regardless of whether there has been a legitimate derogation from the prohibition of the use of force laid down in Article 2 para. 4 UN Charter.[96] The codified legal framework for the IHL consists primarily of four Geneva Conventions for the Protection of War Victims adopted in 1949[97] (hereinafter referred to jointly as "the 1949 Geneva Conventions") and supplemented by two Additional Protocols of 1977: Additional Protocol I (AP I), relating to the protection of victims of international armed conflicts, and Additional Protocol II (AP II), relating to the protection of victims of non-international armed conflicts.[98]

94 Sanz Cabellero, 2023, p. 6.

95 Jordan, 2016, p. 56.

96 According to the International Committee of the Red Cross (ICRC), determination of the existence of an armed conflict and the related applicability of IHL depends on only the circumstances prevailing on the ground and not whether the use of force against another state is permitted under the UN Charter. Whether a state uses force in accordance with its right of self-defence, because it has been authorised to do so by a UN Security Council mandate, or in violation of the prohibition on the use of force, does not affect the determination of the existence of an international armed conflict; ICRC, 2016, para. 215; see also Moussa, 2008.

97 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, adopted in Geneva on 12 August 1949, UN Treaty Series vol. 75, Reg. no. 970; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, adopted in Geneva on 12 August 1949, UN Treaty Series vol. 75, Reg. no. 971; Geneva Convention Relative to the Treatment of Prisoners of War, adopted in Geneva on 12 August 1949, UN Treaty Series vol. 75, Reg. no. 972; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, adopted in Geneva on 12 August 1949, UN Treaty Series vol. 75, Reg. no. 973.

98 Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), adopted in Geneva on 8 June 1977, UN Treaty Series vol. 1125, Reg. no. 17512; Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of non-international armed conflicts (Protocol II), adopted in Geneva on 8 June 1977, UN Treaty Series vol. 1125, Reg. no. 17513.

The nature of hybrid conflicts prompts questions about whether the IHL applies to hybrid threats and warfare and, if yes, to what extent. Hybrid conflicts, by definition, exploit the grey zone threshold of an armed conflict; therefore, they provoke uncertainty as to whether the given use of a hybrid threat or warfare triggers the law of armed conflicts. The issue goes far beyond academic debate, and its practical significance is that it allows one to determine the proper legal framework regulating the conduct of hostilities in the given hybrid conflict. Should the IHL be activated, it influences the application of international human rights law, especially as it affects the interpretation and scope of restrictions of certain rights and freedoms under the general human rights regime (see section 3.3 below). For example, during an armed conflict, adversary combatants become legitimate objects of attack, and civilians who directly participate in hostilities lose their general protection against dangers arising from military operations.[99]

The common Article 2 para. 1 of the 1949 Geneva Conventions provides that the IHL applies to all cases of 'declared war' or of 'any other armed conflicts', even if the state of war is not recognised by one of them. Instead of providing a legal definition, the 1949 Geneva Conventions introduced a fact-based approach to the notion of an armed conflict. By virtue of Article 2 para. 1 of the 1949 Geneva Conventions, IHL is applicable as soon as a state undertakes hostile military action(s) against another state.[100] According to the International Committee of the Red Cross (ICRC), how states characterise the armed confrontation does not affect the application of the 1949 Geneva Conventions if the situation evidences that the concerned state is effectively involved in hostile armed actions against another state. The fact that a state does not, for political or other reasons, explicitly refer to the existence of an armed conflict in a particular situation does not prevent it from being legally classified as such.[101]

The interpretation of the notion of "an armed conflict" under the common Article 2 para. 1 of the 1949 Geneva Conventions refers to military hostilities and armed actions, that is, the prevailing form of waging wars at the time of drafting of the 1949 Geneva Conventions. This approach has been supported by, among others, the International Criminal Tribunal for the Former Yugoslavia (ICTY), which holds that 'an armed conflict exists whenever there is a *resort to armed force* between States or *protracted armed violence* between governmental authorities and organised armed groups or between such groups within a State' (emphasis added).[102] In light of such an interpretation, there is no legal basis to establish that hybrid conflicts that do not involve violent actions trigger the application of the 1949 Geneva Conventions and IHL. Nevertheless, the ICRC has recently begun to consider technological

99 See: Article 51 paras. 1–3 of the AP I.
100 ICRC, 2016, para. 209.
101 Ibid., para. 213.
102 ICTY, *The Prosecutor v. Duško Tadić*, Decision of 2 October 1995 on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-A, para. 70.

advancements, particularly the exponential increase in states' cyber-capabilities and their potential impact on the civilian population and infrastructure, for the applicability of the humanitarian law. According to the ICRC, cyberoperations that have effects similar to classic kinetic operations, result in the destruction of civilian or military assets, or cause the death or injury of soldiers or civilians may amount to an armed conflict within the meaning of Article 2 para. 1 of the 1949 Geneva Conventions, even if they are not carried out in conjunction with classic military operations.[103] From the perspective of IHL, these situations should not be treated as different from equivalent attacks conducted through more traditional means and methods of warfare. Peter Mauer, former President of the ICRC, argues that multiple strategies are needed to adapt IHL to today's hybrid kinetic-cyber realities. He suggests making logical legal interpretations from already existing legal concepts under the 1949 Geneva Conventions, such as the principles of distinction, proportionality, and precaution, arguing that through proper interpretation, it would be possible to make them applicable to cyberoperations in today's conflicts.[104]

Second, the subdivision between international armed conflicts and non-international armed conflicts, underlying the IHL, makes the legal assessment of a hybrid campaign even less straightforward. Based on factual and objective criteria (e.g. involvement of an armed force), if a given hybrid conflict meets the threshold of an armed conflict under common Article 2 para. 1 of the 1949 Geneva Conventions resulting in the activation of the IHL, further classification of the conflict as an international or non-international conflict is required. International armed conflict is understood as an armed conflict between two or more states. By contrast, non-international armed conflicts are restricted to the territory of a single state, involving either regular armed forces fighting groups of armed dissidents or armed groups fighting each other.[105] As Antonio Cassese points out, the division between these two subcategories of armed conflicts has a substantial practical impact: While international armed conflicts are subject to a wide range of rules, including those set out in the four 1949 Geneva Conventions and AP I, internal conflicts are governed only by a limited range of rules (common Article 3 of the 1949 Geneva Conventions and AP II).[106] The distinction is all the more important as non-international armed conflicts are nowadays the most prevalent form of armed conflict.[107]

The existence of an international armed conflict is not dependent on any threshold for the intensity of the armed confrontation or the duration of the hostilities. According to the ICRC, even minor skirmishes between armed (land, air, or

103 ICRC, 2016, para. 255. According to van den Bosch, the view that IHL is applicable below the threshold of attacks is not necessarily limited to cyberoperations and can even be applied to all non-destructive military operations such as information campaigns or disturbing operations such as jamming; van den Bosch, 2021, p. 219.

104 Mauer, 2023.

105 ICRC, 2004.

106 Cassese, 2008, pp. 5–6; ICRC, 2004.

107 ICRC, 2016, para. 194.

naval) forces can spark an international armed conflict and lead to the applicability of the humanitarian law.[108] As already mentioned, the ICRC accepts that cyberoperations having effects similar to classic kinetic operations might also amount to an international armed conflict if they result in the destruction of property or cause the death or injury of soldiers or civilians.

The legal category of non-international armed conflicts is vague and surrounded by legal uncertainties due to the non-defined criteria regarding the level of organisation for the non-state group, geographical scope of the internal armed conflict, and intensity of hostilities and control of territory.[109] Whether the internal hostilities level up to a non-international armed conflict determines the possibility of the use of force. A crisis below the threshold for a non-international armed conflict needs to be managed using national crisis and emergency law as well as law enforcement rules of engagement under a human rights regime. On the contrary, a conflict involving sufficient degree of organisation and intensity of hostilities to prompt the application of *jus in bello* for non-international armed conflicts will allow for more offensive rules of engagement, which, nevertheless, will be more restrictive and defensive than the rules of engagement for a full-scale international armed conflict.[110] Hybrid campaigns provide a fertile ground for circumventing (and abusing) the already uncertain threshold of a non-international armed conflict, making the legal assessment underlying strategic and political decision-making very challenging, especially in situations where hybrid adversaries target multiple states simultaneously with asymmetric means and different intensities.[111]

According to Fogt, the distinction between an international and non-international armed conflict in a hybrid warfare depends on the evidence of state attribution, which is a sensitive and highly political issue.[112] The attribution of hostilities to a given state actor is not without major difficulties, partly because of the state's denial policy and cover operations, which are the essence of hybrid tactics, and partly because of different requirements for state attribution adopted by different international courts. The ICJ upholds a strict requirement for a conduct to give rise to legal responsibility of the state, expecting that it must be proven that that state had "effective control" of the military or paramilitary operations ("effective control test").[113] By contrast, the ICTY has held that the ICJ's effective control requirement was not suitable for acts of organised groups (e.g. a military unit or, in case of war or civil strife, armed bands of irregulars or rebels), where the lower standard of

108 Ibid., paras. 236–237.
109 Fogt, 2020, p. 73.
110 Ibid., p. 74.
111 Ibid.
112 Ibid.
113 ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*, para. 115.

"overall control" can be applied to attribute to a state the acts of such groups.[114] The ICJ's strict requirement of "effective control" legally allows the state to use non-state actors in the grey zone where the standard of attribution cannot be met.[115]

State practice shows that hybrid adversaries tend to conceal their involvement, using various means and methods, to avoid reaching the threshold of an international armed conflict. During the 2014 hybrid conflict, Russia employed unmarked forces (little green men) for its hostile operations in Crimea. Initially, Russian authorities successfully asserted that the little green men comprised persons of Crimean origin and formed part of the Ukrainian self-defence forces. Wentzel argues that, from a tactical viewpoint, the presence or absence of national insignia was of little importance.[116] The principal effect of the absence of national markings and the broader information operations campaign was to bolster Russia's strategic narrative that the events in Crimea were initially domestic in origin. Since, according to the Russian narrative, the little green men were not Russian soldiers, the Russian Federation could maintain plausible deniability of the military operation and disavow their actions within a sovereign state. More importantly, Russia's claim that the little green men were Ukrainian self-defence forces was meant to shift the classification of the conflict from an international conflict to a domestic one. Once labelled a domestic conflict, it was more difficult for Ukrainian authorities to address the international community and request foreign intervention onto its territory.[117] This simultaneously distracted the international community and facilitated Russia's subsequent actions – overt military operations to support the purported self-determination movement and incorporate Crimea into the Russian Federation.

3.3. Human Rights Law

Preventing and countering hybrid threats and warfare goes parallel with the curtailment of certain human rights and freedoms, although the scope of restrictions is limited by international law and depends on legal classification of the hybrid threats. The relevant legal regime regulating restrictions and derogations from human rights standards is anchored in both the international human rights

114 ICTY, *The Prosecutor v. Duško Tadić*, Appeals Chamber Judgment of 15 July 1999, Case No. IT-94-1-A, para. 120.

115 Fogt, 2022, p. 74.

116 Wentzell, 2021, p. 45.

117 Use of the little green men sufficiently concealed the Russian origin of the attack and gave more reluctant members of NATO grounds to debate whether or not an armed attack, rather than domestic unrest, has indeed occurred. Wentzell further argues that from a tactical viewpoint, the presence or absence of national insignia was of little importance. Had they considered the unmarked little green men exclusively as a domestic threat, the Ukrainian armed forces would have been constrained by their domestic legal regime concerning the use of force against their own people. However, it is more likely that upon recognising that there was foreign interference, the rules of IHL would have governed the conflict, and the Ukrainian armed forces would have only been required to distinguish combatants from non-combatants; Wentzell, 2021, pp. 45–47.

law and IHL, and it forms an inherent part of the legal assessment of hybrid threats and warfare. The Council of Europe's Committee of Legal Advisers on Public International Law (CAHDI) recommends that each case of a hybrid campaign must be assessed individually according to the relevant legal regime.[118] While international human rights law is relevant to both military and non-military actions carried out as part of hybrid threats and warfare, if the hybrid actions level up to an armed conflict (be it international or non-international armed conflict), then the IHL also becomes applicable and affects the interpretation and scope of restrictions on human rights and freedoms. In situations of armed conflict, the protections offered by human rights conventions and the IHL co-exist, as highlighted by the ICJ[119] and the European Court of Human Rights (ECtHR).[120] According to the ICJ and ECtHR, the relationship between the IHL and human rights law can unfold according to three scenarios: some rights may exclusively be matters of the IHL, others may exclusively be matters of human rights law, and some others may be matters of both these branches of international law.[121]

From the perspective of the European Convention on Human Rights (ECHR),[122] use of a hybrid threat and warfare would prompt different consequences depending on whether it occurs (1) in times of war, (2) in times of a public emergency other than war, or (iii) in peacetime when no armed conflict or public emergency exists.

According to Article 15 para. 1 ECHR, in times of "war" or "other public emergency" threatening the life of a nation, states may derogate from their obligations under the ECHR.[123] The formal condition for a valid derogation is an official declaration of the state of emergency by law at the domestic level.[124] Article 15 para. 2 ECHR excludes the possibility of derogation, even under a

118 CAHDI, 2018, para. 3.

119 ICJ, *Legality of the Threat or Use of Nuclear Weapons,* para. 25. See also ICJ, *The Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, para. 106; ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of Congo (DRC) v. Uganda*, judgment of 19 December 2005, para. 216.

120 ECtHR, *Hassan v. the United Kingdom*, judgement of 16 September 2014, Application No. 29750/09, paras. 102–103. In the past, the IHL framework was considered *lex specialis* to the human rights framework; nowadays, however, it is accepted that both legal areas are applicable at the same time and mutually influence each other's application.

121 ICJ, *The Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, para. 106; ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of Congo (DRC) v. Uganda*, judgement of 19 December 2005, para. 216; ECtHR, *Hassan v. the United Kingdom*, para. 102.

122 *Convention for the Protection of Human Rights and Fundamental Freedoms*, adopted in Rome on 4 November 1950, ETS No. 005 (hereinafter referred to as ECHR).

123 Article 15 para. 1 ECHR states that
In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.

124 Council of Europe, 2022, para. 53.

state of emergency, with respect to the right to life (Article 2 ECHR), prohibition of torture (Article 3 ECHR), prohibition of slavery or servitude (Article 4 para. 1 ECHR), and prohibition of punishment without law (Article 7 ECHR). Further non-derogable rights stem from additional Protocols to the ECHR (the right to *ne bis in idem*, as well as the protection against the death penalty),[125] while some rights are considered non-derogable, even if they are not expressly specified in the ECHR or its Protocols (e.g. the right to a fair trial and the right to an effective remedy).[126]

Based on Article 15 para. 2 ECHR, lawful use of force validates derogations from the otherwise non-derogable right to life. Deaths resulting from lawful acts of war constitute an exemption from the absolute protection under Article 2 ECHR. By the same token, the non-derogable status of the prohibition of death penalty does not exclude capital punishment in respect of acts committed in times of war or imminent threat of war.[127] The ECtHR is not required to interpret the meaning of "war" in Article 15 para. 1 ECHR. According to the prevailing view, the term "war", enabling far-reaching derogations from human rights under Article 15 paras. 1–2 ECHR, should be understood as an "armed conflict" (international or non-international) within the meaning of the common Article 2 of the 1949 Geneva Conventions.[128] Schabas suggests that it should be interpreted in light of the test used by the ICTY in the *Tadić* case, which implies that a "war" within the meaning of Article 15 para. 1 ECHR exists whenever there is a resort to armed force or protracted armed violence.[129] By referencing the understanding of "armed conflict" under the IHL, it seems justified to conclude that hybrid hostilities can activate the most far-reaching derogations from human rights if they involve the use of armed force, or *mutatis mutandis*, resulting in the destruction of civilian or military assets or death or injury of soldiers or civilians, even if they are not carried out in conjunction with classic military operations (see section 3.2 above). If a hybrid campaign meets the threshold of an armed conflict, it has two consequences: (1) derogation from Article 2 ECHR is allowed, and (2) the IHL becomes applicable as *lex specialis* to the international human rights law and determines if the lethal use

125 Article 3 of Protocol No. 6 to the Convention for the Protection of Human Rights and Fundamental Freedoms concerning the Abolition of the Death Penalty, ETS No. 114; Article 2 of Protocol No. 13 to the Convention for the Protection of Human Rights and Fundamental Freedoms, concerning the abolition of the death penalty in all circumstances, ETS No. 187); and Article 4 para. 3 of Protocol No. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 117.

126 Council of Europe, 2022, paras. 71–75.

127 Article 2 of Protocol No. 6 to the Convention for the Protection of Human Rights and Fundamental Freedoms concerning the Abolition of the Death Penalty.

128 Fogt, 2020, p. 94.

129 See: ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*, para. 115; Schabas, 2015, pp. 594–595.

of force is lawful.[130] Similarly, the existence of an armed conflict triggering the application of the IHL also affects the interpretation of the provisions of Article 5 ECHR (right to liberty and security). This can occur only in cases of international armed conflict, where the taking of prisoners of war and detention of civilians who pose a threat to security are accepted features of the IHL, and Article 5 ECHR could be interpreted as permitting such broad powers.[131]

A public emergency other than war that allows states to derogate from human rights, although not from the Article 2 of the ECHR, covers exceptional situations of crisis or emergency that affect the whole population and constitute a threat to the organised life of the community.[132] To enable derogations from human rights obligations under Article 15 para. 1 ECHR, the effects of a crisis situation must be actual or imminent, must involve the whole nation, and threaten the continuance of organised life of the community; moreover, the crisis or danger should be exceptional, meaning that normal measures or restrictions, permitted by the ECHR for public safety, health, and order, must be inadequate.[133] Following the terrorist attacks of 11 September 2001, the ECtHR has taken the stand that the requirement for public emergency under Article 15 para. 1 ECHR (a threat to the life of the nation) does not need to be understood narrowly as a threat of serious physical damage and loss of life, but it can extend to a menace to the institutions of government or the existence of a civil community.[134] Not every public emergency constitutes a threat to the life of the nation to justify derogations from the ECHR; however, states enjoy a wide margin of appreciation in assessing whether the life of nation is threatened by a public emergency and can consider a

130 Fogt, 2020, p. 94. The ICJ's 1996 *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons* contains a good illustration of the interplay between human rights and IHL with respect to the right to life. While considering whether the use of nuclear weapons violates the right to life guaranteed in Article 6 para. 1 International Covenant on Civil and Political Rights, the ICJ concluded that

> The protection granted by the International Covenant on Civil and Political Rights does not cease in times of war, except by virtue of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency. Respect for the right to life is not, however, such a provision. In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities. The test of what is an arbitrary deprivation of life, however, then falls to be determined by the applicable lex specialis, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities. Thus, whether a particular loss of life, through the use of a certain weapon in warfare, is to be considered an arbitrary deprivation of life contrary to Article 6 of the Covenant, can only be decided by reference to the law applicable in armed conflict and not deduced from the terms of the Covenant itself.

See: ICJ, *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, para. 25.

131 *Hassan v. United Kingdom*, paras. 102–105.

132 ECtHR, *Lawless v. Ireland (no. 3)*, judgement 1 July 1961, Application No. 332/57, para. 28.

133 The test applied to assess whether a situation constitutes a public emergency threatening the life of the nation was formulated by the ECHR in the "Greek Case": Denmark, Norway, Sweden, Netherlands v. Greece, Applications Nos. 3321/67, 3322/67, 3323/67, 3344/67, opinion of the Sub-Commission, 4 October 1969; see also Schabas, 2015, p. 595.

134 ECtHR, A. *and Others v. the United Kingdom*, judgement of 19 February 2009, Application No. 3455/05, para. 179.

broad range of factors in determining the nature and degree of the actual or imminent threat.[135] The hybrid threat or warfare below the threshold of an armed conflict could become a valid ground for derogation from the ECHR obligations if it created a public emergency involving an actual or imminent threat to the existence of the nation. In such a case, safeguards under the ECHR would continue to apply, subject to possible derogations, which nevertheless could not encompass the safeguards under Articles 2, 3, and 4 paras. 1 and 7 of the ECHR. In situations short of armed conflict, the IHL framework as such would not be applicable.

The state practice of derogating from their ECHR obligations in times of public emergency can be exemplified by the notifications made by Ukraine following the Russian intervention in 2014. Ukraine derogated from the ECHR (and the International Covenant on Civil and Political Rights [ICCPR]) for the first time in June 2015 on the grounds of the international armed conflict ongoing on its territory since 2014. Since the first notification, more than 20 further derogation notifications have been filed, reflecting the evolution of the armed conflict between Ukraine and Russia.[136] The initial notifications were made in the context of hybrid conflict culminating in the annexation of Crimea, while the notifications made from March 2022 onwards took place in the context of a full-scale armed conflict. Ukraine authorities justified their first derogations in June 2015 with the needs of the anti-terrorist operations conducted by Ukrainian forces in certain areas of the country (Donetsk and Luhansk) against armed aggression from the Russian Federation.[137] Initially, Ukraine exercised the right of derogation from its obligations established in Article 5 (right to liberty and security), Article 6 (right to a fair trial), Article 8 (right to respect for private and family life), and Article 13 (right to an effective remedy) ECHR, as well as in Article 2 para. 3 and Articles 9, 12, 14, and 17 ICCPR. Later, Ukraine derogated from several other human rights obligations under the ECHR and ICCPR as well.[138] Some of the derogations were considered void, as they effected non-derogable rights, either *expressis verbis* based on the ECHR and its Protocols or based on customary international law (e.g. the right to *ne bis in idem*, right to an effective remedy, or right to a fair trial).[139] According to the Council of Europe's interpretation, this does not invalidate Ukrainian derogation as a whole, which remains valid, but only that part of the rights for which the derogation is allowed.[140] The non-derogable rights, even if derogated from, continue to apply, meaning that derogation does not affect these rights and cannot be used to interfere with them. The Ukrainian derogations from human rights obligations complied with the formal conditions under Article 15 para. 1 ECHR, considering that

135 Ibid., paras. 179–180; see also Schabas, 2015, pp. 595–596.

136 For a detailed analysis of Ukraine's derogations from its human rights obligations, see Council of Europe, 2022, p. 2.

137 Secretariat General, 2015.

138 *Legal Analysis of the derogation made by Ukraine under Article 15 of the European Convention of Human Rights and Article 4 of the International Covenant on Civil and Political Rights*, para. 82.

139 Ibid., paras. 71–75.

140 Ibid., para. 80.

when declaring the derogation and state of emergency, Ukraine relied on its national laws. For example, Ukraine relied on Resolution No. 462-VIII of the Verkhovna Rada in the June 2015 notification, on amendments to several national laws implementing specific derogatory measures in 2016, and on martial law declaring an emergency and imposing derogatory measures since February 2022.[141]

All notifications on derogations filed by Ukraine since 2015 referred to one ground for the derogation – armed aggression of the Russian Federation. In the 2015 notification, Ukraine referred to the annexation and temporary occupation by the Russian Federation of the integral part of Ukraine – the Autonomous Republic of Crimea and the city of Sevastopol – as a result of armed aggression against Ukraine, involving 'both regular Armed Forces of the Russian Federation and illegal armed groups guided, controlled and financed by the Russian Federation'.[142] The 2022 notifications referred to 'military aggression of the Russian Federation against Ukraine' as grounds for derogation.[143] Although the 2014 Russian-Ukrainian conflict is considered an archetypical example of a hybrid campaign, the derogations notified in 2015 were substantiated by the existence of an armed aggression and not by the use of non-kinetic means also widely employed in the conflict. Although the Ukrainian case-study is not the most apposite example of a derogation under Article 15 ECHR for a hybrid threat and warfare not involving military means, it showcases the practical functioning of the derogation clause in the context of a hybrid campaign. It has been suggested that in the 2021 migration crisis on the Polish/Latvian/Lithuanian-Belarussian border, which was considered to involve hybrid attacks that used coercive engineered migration, invoking the derogation clause under Article 15 ECHR could have been a viable option for the targeted states, especially considering that all three of them invoked public emergency measures. A situation of instrumentalised migration could be qualified as a public emergency where the situation reaches the level of prohibited use of force and validates the derogation from human rights obligations.[144]

The third possible scenario involving the effect of hybrid actions under the human rights framework refers to situations where the hostilities do not amount to armed conflict or a public emergency threating the nation. The derogation clause in Article 15 ECHR is not applicable, nor is the IHL.[145] In peacetime, no derogation from human rights obligations is possible, while restrictions on human rights and freedoms guaranteed in the ECHR can be imposed only in accordance with the limitation clauses specifically provided for in the ECHR. In accordance with para. 2 of Articles 8, 9, 10, and

141 Ibid., paras. 58–59.

142 *Notification – JJ7979C Tr./005-185 – Ukraine – Derogation to the Convention on the Protection of Human Rights and Fundamental Freedoms*, p. 2.

143 Secretariat General, 2022, p. 3.

144 Huttunen, 2024.

145 Nevertheless, according to the ECtHR, lack of a formal derogation under Article 15 of the ECHR does not prevent the court from considering the context and provisions of IHL when interpreting and applying the ECHR rights in peacetime, e.g. Article 5; see: *Hassan v. United Kingdom*, para. 104.

11 ECHR, as well as Article 2 para. 3 of Protocol No. 4 to the ECHR,[146] the protection of national security or public safety can constitute valid grounds for curtailment of human rights. Any response to hybrid threats and warfare leading to human rights restrictions must not only pursue a legitimate aim, such as national security, but also be prescribed by law and be necessary in a democratic society. Moreover, Article 18 ECHR prohibits the states from applying the restrictions permitted under the ECHR for any purpose other than those for which they have been prescribed.

The Parliamentary Assembly of the Council of Europe has expressed a concern that certain Member States have already taken measures (e.g. surveillance measures, blocking of websites, expulsion of foreigners, and criminal convictions for online statements) that prompt questions concerning the respect for human rights, primarily the right to freedom of expression, along with the right to information, right to respect for one's privacy, and right to the freedom of movement.[147] A 2018 Recommendation of the Parliamentary Assembly envisaged the development of new legal standards to prevent and combat hybrid threats and warfare, which was followed by a Parliamentary Assembly resolution with that aim.[148] However, the CAHDI considered that developing new legal standards to prevent and combat the threats of "hybrid war" is premature at this stage, considering the absence of a common understanding as to what a "hybrid war" is.[149]

When considering hybrid threats and warfare from the perspective of the international human rights law, it is exceedingly difficult to balance the interests of national security and states' sovereignty with freedom of expression, right to privacy, and other individual human rights and freedoms. That combined with the legal asymmetry between hostile actors and democratic states and the fear of eventual "hypocrisy costs"[150] can hamper an effective response to hybrid threats; this further enhances the likelihood of the success of hybrid actions. The human rights agenda,

146 Protocol 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms, securing certain Rights and Freedoms other than those already included in the Convention and in the First Protocol thereto, signed on 16 September 1963, ETS No. 46.

147 Parliamentary Assembly of the Council of Europe, *Legal challenges related to hybrid war and human rights obligations*, Resolution 2217 (2018).

148 Parliamentary Assembly of the Council of Europe, Recommendation 2130 (2018) on the 'Legal Challenges Related to Hybrid War and Human Rights Obligations', 26 April 2018; Parliamentary Assembly of the Council of Europe, *Legal challenges related to hybrid war and human rights obligations*, Resolution 2217 (2018).

149 *Opinion of the CAHDI On Recommendation 2130 (2018) of the Parliamentary Assembly of the Council of Europe – 'Legal Challenges Related to Hybrid War and Human Rights Obligations'*, para. 5.

150 The term "hypocrisy costs" denotes symbolic political reputational costs that can be imposed when there exists a real or perceived disparity between a professed commitment to liberal values and/or international norms and demonstrated state actions that contravene such a commitment. They are operationalised in a manner such that once a government or its leadership has publicly committed itself to a principle, canny observers can use those positions, and their command of information, to expose the distance between discourse and practice. Hypocrisy costs can further enhance the likelihood of success of hybrid actions carried out by hybrid adversaries; for an example of coercive engineered migration, see: Blake-Martin, 2023.

which questions absolute state sovereignty, might at times collide with the UN Charter and has been identified as a major challenge to the international security architecture.[151]

4. Legal Assessment Under the EU Law and Policies

4.1. Hybrid Threats within the EU Common Defence and Security Policy

Countering of hybrid threats forms an integral part of the Strategic Compass for Security and Defence, the first quasi-military strategy of the EU approved by the Council of the EU on 21 March 2022. It establishes a common strategic vision for the EU's security and proposes several concrete actions in four main domains: act, secure, invest, and partner. The action plan under the Strategic Compass sets out, among others, main objectives related to countering hybrid threats. These include the (1) creation of the EU Hybrid Toolbox, consisting of various instruments to prepare for and respond in a coordinated manner to a wide spectrum of hybrid threats; (2) creation of the Hybrid Fusion Cell to enhance situational awareness through strategic analysis and assessments of hybrid threats; and (3) establishment of the EU Hybrid Rapid Response Teams to secure short-term and targeted assistance to EU Member States in case of a hybrid campaign.[152] Moreover, the Strategic Compass envisages measures to counter foreign information manipulation and interference (FIMI) taking place within broader hybrid campaigns, such as by developing the EU toolbox to address and counter the FIMI. These actions are to be implemented in parallel to enhance further counter-hybrid cooperation with NATO.

The significance attributed to countering hybrid threats, evidenced by its fully-fledged place in the Strategic Compass, is a consequence of several years of policymaking for hybrid threats long preceding the adoption of the Strategic Compass. The EU's policymaking for addressing hybrid threats began in the aftermath of the 2014 Russian annexation of Crimea and the beginning of the Donbas conflict. In 2015, the Council of the EU adopted conclusions on the Common Defence and Security Policy, calling for a joint framework with actionable proposals to counter hybrid threats and foster the resilience of the EU and its Member States. The first comprehensive policy document, the *Joint Framework on Countering Hybrid Threats – A European Union Response*[153] was issued in 2016 by the European Commission and High Representative

151 Hathaway, 2014, pp. 217–222; Sanz Caballero, 2023, p. 5.

152 Strategic Compass for Security and Defence, 2022, p. 22.

153 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response*, Brussels, 6 April 2016, JOIN(2016) 18 final.

of the Union for Foreign Affairs and Security Policy; this was followed by the 2016 EU *Operational Protocol for Countering Hybrid Threats 'EU Playbook'*[154] and the *2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Counter Hybrid Threats*.[155] In 2020, a mapping of almost 200 measures related to enhancing the EU's resilience against hybrid threats, implemented under the auspices of the EU, was made public.[156] A highly relevant policy document, the *Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns*,[157] was adopted in June 2022 to support the development of the EU Hybrid Toolbox and counter the FIMI actions as envisaged in the 2022 Strategic Compass. These conclusions have been adopted in light of Russia's armed aggression against Ukraine, which, as the Council of the EU acknowledged, was 'combined with hybrid tactics, cyberattacks, foreign information manipulation and interference, economic and energy coercion and an aggressive nuclear rhetoric'.[158] The *Annual Progress Report on the Implementation of the Strategic Compass for Security and Defense*, published in March 2023, recognised that the use of hybrid tactics against the EU and its Member States has been exacerbated by Russia's invasion of Ukraine, which has witnessed hybrid tactics such as the instrumentalisation of food, irregular migration, energy, and lawfare.[159]

4.2. Coordinated and Collective Response to Hybrid Threats under the EU Legal Framework

The primary responsibility for countering hybrid threats and campaigns relates to national security and defence and lies with the EU Member States. Nonetheless, many Member States face similar or common threats that target cross-border infrastructures or networks and can be addressed more efficiently with a coordinated response at the EU level, using instruments envisaged by the EU treaties and policies. The 2016 *Joint Framework on Countering Hybrid Threats – A European Union Response* and the 2022 *Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns* provide an overview of the instruments and policies that are most suitable for a coordinated response to malicious hybrid activities at the EU level.

154 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Staff Working Document. EU operational protocol for countering hybrid threats 'EU Playbook'*, Brussels, 5 July 2016, SWD(2016) 227 final.

155 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council and the Council. Increasing resilience and bolstering capabilities to counter hybrid threats*, Brussels, 13 June 2018, JOIN(2018) 16 final.

156 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Staff Working Document. Mapping of measures related to enhancing resilience and countering hybrid threats*, Brussels, 24 July 2020, SWD(2020) 152 final.

157 Council of the European Union, *Council Conclusions on a Framework for a coordinated EU response to hybrid campaigns*, Brussels 21 June 2022, 10016/22.

158 Ibid., para. 1.

159 High Representative of the Union for Foreign Affairs and Security Policy, 2023, p. 11.

Decisions on a coordinated EU response should be made on a case-by-case basis, and several guiding principles must be observed, as laid down in the 2022 Council Conclusions. The coordinated countermeasures in response to hybrid campaigns should serve to protect democratic values, processes, and institutions, as well as the integrity, security, and strategic interests of the EU, its Member States, and their citizens; they need to provide for attainment of the objectives of the EU, particularly the Common Foreign and Security Policy objectives set out in the Treaty on EU (TEU) and Treaty on the Functioning of the EU (TFEU); they shall be based on a shared situational awareness among the Member States and correspond to the needs of the specific situation at hand; and finally, they should consider the broader context of the EU's external relations with the state concerned by the response. More importantly, if seen from the legal perspective, the decision on a coordinated EU response shall ensure that the envisaged countermeasures (1) 'respect international law', (2) 'protect fundamental rights and freedoms', (3) 'support international peace and security', and (4) are '*proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact* of each particular hybrid campaign' (emphasis added).[160]

In many cases, a decision on a lawful and proportionate response to hybrid campaigns is contingent on the attribution. The process of attribution, most importantly legal and political attribution, is understood as assigning responsibility for a malicious hybrid activity to a specific state or non-state actor and consists of different levels.[161] Under the existing EU framework, the attribution is a sovereign national prerogative, a political decision made by EU Member States on a case-by-case basis.[162] The Member States' decision on attribution should be based on all-source intelligence, in which they can rely on the assistance of the EU Single Intelligence and Analysis Capacity framework, which combines civilian and military intelligence to produce all-source intelligence assessments, particularly the Hybrid Fusion Cell. However, hybrid threats and campaigns are often designed in such a way as to create ambiguity around their origins and hinder decision-making processes, which makes attribution a principal legal challenge impeding EU Member States' effective response. In the 2022 Council Conclusions, the Council of the EU affirmed that not all measures forming part of a coordinated EU response to hybrid campaigns require assigning responsibility to a state or non-state actor.[163] Measures covered by the Framework for a Coordinated EU Response can be tailored to the degree of certainty that can be established in each case. When coordinated attribution is not possible or public attribution is not in the best interest of the EU and its Member States,

160 *The EU Framework for a Coordinated Response to Hybrid Campaigns*, para. 8.

161 Some types of hybrid threats also require a technical attribution, such as in case of cyber-incidents, where the process of technical attribution involves using information technology forensics to evaluate technical artefacts and evidence to gather knowledge about the attacker's actions; see: Bendiek and Schulze Attribution, 2021, p. 10.

162 Council conclusions of a Framework for a coordinated EU response to hybrid campaigns, paras. 14 and 17.

163 Ibid., para. 18.

well-calibrated asymmetric actions from the toolbox covered by the framework can be implemented on a case-by-case basis, providing that they comply with international law and receive due approval.[164]

According to the Council of the EU's conclusions, when the perpetrator of a hybrid campaign can be identified "with a high degree of certainty", asymmetric and proportionate measures in line with international law may be taken, to either prevent or respond to a hybrid campaign.[165] Member States' response is not limited to hybrid campaigns that are classified as internationally unlawful acts; they can also be triggered by malicious activities that do not classify as such but are considered unfriendly acts.[166] The EU toolbox includes various countermeasures in areas such as diplomatic, political, military, economic, and strategic communication. Countermeasures based on the Framework on a Coordinated EU Response to hybrid threats can encompass measures falling within the foreign, security, and defence policy, such as (1) preventive measures, including capacity and confidence building measures; (2) cooperative measures, (3) stability building measures, including public diplomacy and diplomatic engagement with the involved state actor; (4) restrictive measures (sanctions); and (5) measures to support Member States, upon their request, which choose to exercise their inherent right of individual or collective self-defence as recognised in Article 51 UN Charter.[167] Category 5 refers to collective defence under the mutual assistance clause in Article 42 para. 7 TEU[168] and the solidarity clause under Article 222 TFEU.[169]

The solidarity clause, laid down in Article 222 TFEU, provides that the EU and its Member States can act jointly in a spirit of solidarity if a Member State is the object of "a terrorist attack" or victim of a "natural or man-made disaster".[170] Article 222 TFEU allows for an EU action as well as direct assistance by one or several Member States to a targeted Member State.[171] EU action under Article 222 para. 1 TFEU is implemented

164 Ibid.

165 Ibid., para. 14.

166 Ibid.

167 Ibid., paras. 14–15. The objective of measures within foreign, security, and defence policy are to strengthen prevention, encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term.

168 *Treaty on European Union of 13 December 2007* – consolidated version, Official Journal of the European Union C/202 of 7 June 2016.

169 *Treaty on the Functioning of the European Union of 13 December 2007* – consolidated version, Official Journal of the European Union C/202 of 7 June 2016.

170 Both terms are defined in Article 3 of Council Decision 2014/415/EU. A "terrorist attack" means a terrorist offence as defined in Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, while "disaster" means any situation that has or may have a severe impact on people, the environment, or property, including the cultural heritage.

171 The solidarity clause was introduced by the Treaty of Lisbon as a political response to different terrorist attacks, such as those in New York in 2001 and Madrid in 2004, as well as to natural disasters such as the floods in Central Europe in 2002. The location of Article 222 TFEU in Part V TFEU concerning the external action by the EU underlines that the sources of these threats are, at least in part, seen to be outside the EU, even though the events dealt with in Article 222 TFUE occur on the territory of the Member States and not externally; see: Erlbacher, 2019, p. 1691.

by applying Council Decision 2014/415/EU,[172] which sets out the conditions of invocation of the solidarity clause and the available means of reaction. The solidarity clause is designed as a subsidiary tool of last resort, as the affected Member States may invoke it only if they consider that the crisis clearly overwhelms the response capabilities available to them, after having exploited the possibilities offered by existing means and tools at the national and EU levels.[173] The affected Member State addresses the invocation of Article 222 TFUE to the Presidency of the Council of the EU. The European Commission and EU High Representative identify the relevant EU instruments that can best contribute to the response to the crisis. In their respective areas of competence, they are both responsible for taking all the necessary measures provided under those instruments, identifying military capabilities with the support of the EU Military Staff, identifying and proposing the use of instruments and resources falling within the remit of EU agencies, and producing regular integrated situational awareness and analysis reports.[174] Invocation of the solidarity clause triggers coordination at the Council of the EU level (Integrated Political Crisis Response arrangements).[175] Application of the solidarity clause under Article 222 para. 1 TFEU stems from the EU's general obligation of solidarity towards its Member States, expressed as the obligation to mobilise all instruments at its disposal, including the military resources made available by the Member States, to assist a Member State at the request of its political authorities in the event of a terrorist attack, to protect democratic institutions and the civilian population from any terrorist attack, and to prevent the terrorist threat in the territory of the Member States. In situations involving direct assistance by one or several Member States to a Member State under Article 222 para. 2 TFUE, Council Decision 2014/415/EU does not apply. The obligation of mutual assistance between Member States is expressed in a less extensive manner than the solidarity obligation incumbent on the EU towards its Member States. Each Member State has the sovereign right to choose the most appropriate means to comply with its own solidarity obligation towards the affected Member State.[176]

If a hybrid attack includes an armed aggression, it can trigger the invocation of the mutual assistance clause (also referred to as the mutual defence clause) set forth in Article 42 para. 7 TEU. It guarantees that

> If a Member State is the victim of *armed aggression* on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. (emphasis added)

172 Council Decision 2014/415/EU of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause, Official Journal of the European Union, 1 July 2014, L 192/53.
173 Article 4 para. 1 of Council Decision 2014/415/EU.
174 Article 5 para. 2 of Council Decision 2014/415/EU.
175 Joint Framework on countering hybrid threats, p. 16.
176 Declaration No. 37 on Article 222 of the Treaty on the Functioning of the European Union, Official Journal of the European Union, 7 June 2016, C 202/349.

Article 42 para. 7 TEU imposes a legally binding obligation on Member States to provide 'aid and assistance by all the means in their power' to a Member State that is the victim of armed aggression in its territory. However, the exact nature of aid and means of assistance can be determined by each Member State differently. Article 42 para. 7 TEU does not require Member States to take military action; military assistance remains only one possible means of aid.

Unlike the solidarity clause under Article 222 TFEU, the mutual assistance clause foresees Member States' action only, providing for a direct country-to-country support, without a previously determined procedure of implementation that needs to be followed. Member States implement the mutual assistance clause bilaterally with the Member State invoking it, which, at least in theory, allows for a prompter, more flexible, and tailored response.[177] Any cooperation between the Member States under Article 42 para. 7 TEU should respect the specific character of the Member States' security and defence policy and comply with the commitments under the NATO, which remains the foundation of its member states' collective defence and the forum for its implementation.[178] As Ramopoulos notes, insertion of Article 42 para. 7 TUE in the text of the Treaties does not transform the EU into a defence or military alliance but instead conveys a strong political message.[179]

The key question from the point of view of legal assessment of hybrid threats and warfare from the perspective of EU law is whether and when hybrid operations can be classified as an armed aggression under Article 42 para. 7 TEU or a terrorist attack or man-made disaster under Article 222 TFEU to enable a collective response. EU policy papers confirm that "multiple serious hybrid threats" can amount to armed aggression and thus fall within the ambit of Article 42 para. 7 TEU.[180] However, it is believed that the solidarity clause is more likely to be used in the case of hybrid attacks that combine criminal and subversive actions without military means.[181] The Council of the EU has recognised that while the use of military force can be an integral component of some state actors' hybrid tactics, they might also use hybrid tactics as a substitute for armed aggression.[182]

177 Ramopoulos, 2019, p. 282; see also Nováky, 2017.

178 Council conclusions of a Framework for a coordinated EU response to hybrid campaigns, para. 15.

179 Ramopoulos, 2019, p. 282.

180 *Joint Framework on countering hybrid threats*, p. 16. For a recent study on the applicability of Article 42 para. 7 in response to hybrid threats, see: Deen, Zandee and Stoetman, 2022.

181 European Commission and The High Representative of the Union for Foreign Affairs and Security Policy, *Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – European Union response*, Brussels, 19 July 2017, JOIN(2017) 30 final, p. 16. The practice shows that states might be more willing to invoke Article 42 para. 7 TEU than Article 222 TFEU, even when the underlying crisis is not of a military nature, due to the more flexible and less regulated framework of mutual assistance compared to the solidarity clause, which does not entail handing over of political coordination to the Council Presidency, as in the procedure of Article 222 para. 1 TFEU. Nevertheless, any definite conclusions cannot be well-founded, as Article 42 para. 7 TEU has so far been invoked only once, by France in 2015, following the terrorist attacks in Paris. For more, see Bakker et al., 2016, pp. 22–29.

182 Council conclusions of a Framework for a coordinated EU response to hybrid campaigns, para. 16.

The 2016 *Joint Framework on Countering Hybrid Threats* has called on the European Commission and EU High Representative to examine the applicability and practical implications of Article 222 TFEU and Article 42 para 7 TEU in case a wide-ranging and serious hybrid attack occurs, but such an assessment has not been accomplished yet. A clearer specification of the thresholds for and consequences of invoking either clause in the event of a hybrid threat could significantly enhance the EU's ability to promptly counteract hybrid hostilities in line with the common operational protocol. Although embarking on negations on purely hypothetical thresholds would be counterproductive, creating a common frame of reference among EU Member States through regular simulations and joint exercises could prevent situations where some states could question the legitimacy of the invocation and subsequently refrain from rendering meaningful assistance.[183]

So far, the Member States' practice does not provide any examples of invoking either the mutual assistance or solidarity clause to counter hybrid threats. The artificially engineered migration surge on the Poland-Belarus, Lithuania-Belarus, and Latva-Belarus borders in 2021, identified by EU officials as hybrid attacks, was dealt with by the affected countries without resorting to either Article 42 para. 7 TEU or Article 222 TFEU. The three targeted countries successfully managed the hybrid attacks with domestic crisis regulations on public emergency,[184] and they were supported by the EU's restrictive measures imposed on Belarus. So far, it has been argued that the EU's response to hybrid threats and warfare remains overly circumspect, as the EU is deferring, on the one hand, to national governments to protect themselves and to NATO on the other.[185]

5. Conclusions

In 1952, Hersch Lauterpacht famously wrote that 'if international law is, in some ways, at the vanishing point of law, the law of war is, perhaps even more conspicuously, at the vanishing point of international law'.[186] If the law of war is already at the vanishing point of international law, the emergence of hybrid threats and warfare has pushed it even further into the abyss, for which military and legal scholars have coined the term "grey zone." Waging war with a hybrid arsenal makes contemporary conflicts an alternative example of the Schrödinger's cat paradox, which pins down the dilemma wherein war exists and at the same time it does not. One may argue

183 Deen, Zandee and Stoetman, 2022, p. 22.
184 For an extensive study of the domestic regulations on the public emergency regime in these states, which enabled an effective response to hybrid threats, see: Nagy and Horváth, 2020.
185 Tallis and Šimečka, 2017, pp. 21–22.
186 Lauterpacht, 1952, p. 382.

that unlike the paradox in Schrödinger's quantum experiment, this contradiction can be easily resolved by distinguishing war in the material sense, meaning factual hostilities between states (*de facto* combat), and war in the technical sense, which denotes the normative condition of the state of war (*de jure* state of war).[187] However, the hybrid incidents the world has witnessed in the last two decades, as well as the legal and military debate surrounding them, clearly show that the legal and political assessment of hybrid conflicts is far from that easy.

When assessed in relation to the prohibition of the threat and use of force (Article 2 para. 4 UN Charter) and the right to self-defence (Article 51 UN Charter), hybrid campaigns highlight several specific challenges that the use of unconventional contemporary warfare poses to the international system of war prevention. Prohibition of the use of force under Article 2 para. 4 UN Charter refers to armed force; therefore, classifying hybrid campaigns that do not involve violent military acts as illegal use of force is contrary to the prevailing interpretation of Article 2 para. 4 UN Charter, although some consideration has recently been given to the weapon-like destructive potential of cyberattacks. The threshold for an armed attack enabling the right to self-defence under Article 51 UN Charter is higher than that required to consider hostilities as illegal use of force under Article 2 para. 4 UN Charter; therefore, it is even more difficult to conclude that the use of hybrid threats and warfare would trigger the right to self-defence. Hybrid adversaries deliberately act at such a level of intensity that normally does not allow the targeted state to use forcible measures in self-defence. In the aftermath of the 2014 Russian hybrid operation in Ukraine, the NATO declared that hybrid operations could reach the level of armed attack that could lead to the invocation of Article 5 NATO Treaty. However, it is not clear whether such operations would require any violent acts by hybrid adversaries to trigger the NATO's collective defence mechanism. Otherwise, states targeted with hybrid threat or warfare below the threshold of an armed attack are limited in their response to non-forcible countermeasures and peacetime regulations.

The nature of hybrid conflicts, which combine kinetic and non-kinetic means of warfare, makes it difficult to determine whether the use of hybrid threats and warfare qualifies as an armed conflict that activates the application of IHL, and if yes, whether it triggers the IHL regime for an international or non-international armed conflict. The 1949 Geneva Conventions were drafted at a time when kinetic warfare prevailed, and currently there is no legal basis to establish that hybrid conflicts, which do not involve violent actions, trigger the application of the 1949 Geneva Conventions. Nevertheless, the ICRC has recently begun considering the technological advancements and impact of cyber-capabilities for the applicability of humanitarian law. The experience of the 2014 hybrid conflict between Russia and Ukraine shows that the threshold enabling the application of the IHL for an international armed conflict can easily be averted. The international community's reluctance to declare the existence of an international armed conflict, entailing the risk

187 Dinstein, 2011, pp. 9–10; Greenwood, 1987, p. 283; Lauterpacht, 1968, p. 65.

of escalating violence and possibly activating collective self-defence, can successfully be exploited by hybrid adversaries by using hybrid threats and warfare, such as the use of unmarked forces and the denial policy.

When countering hybrid threats and warfare, states are bound to respect human rights law. The relevant legal regime regulating restrictions on and derogations from human rights obligations is anchored in both the international human rights law and the IHL, and it needs to be assessed individually on a case-by-case basis. Hybrid campaigns can prompt different consequences depending on whether they occur (1) in times of armed conflict, (2) in times of public emergency other than armed conflict, or (3) in peacetime when no armed conflict or public emergency exists. In times of war or other public emergencies threatening the life of the nation, states may derogate from their human rights obligations pursuant to Article 15 ECHR. During armed conflict, the ECHR enables the most far-reaching derogation of human rights, even from the otherwise non-derogable right to life set forth in Article 2 ECHR. In times of public emergencies other than armed conflict, states can derogate from certain human rights obligations, although not from Article 2 ECHR. Hybrid threats or warfare below the threshold of an armed conflict can become a valid ground for derogation from the ECHR regime if the triggering public emergency involves an actual or imminent threat to the existence of the nation and when the normal restrictions permitted by the ECHR for the interests of national security are inadequate. Hybrid hostilities that do not amount to armed conflict or a public emergency threating the life of the nation cannot legitimise any derogations from the human rights obligations under the ECHR. Any response to hybrid threats and warfare entailing restrictions on the enjoyment of individual human rights and freedoms need to be prescribed by law, must pursue a legitimate aim (e.g. interests of national security), and should be necessary in a democratic society. Countering hybrid threats and warfare under the international human rights law paradigm highlights that the main challenge is balancing the interests of national security and state sovereignty with the enjoyment of individual human rights, such as the right to privacy.

In the EU domain, hybrid threats and campaigns can trigger various measures envisaged in the EU treaties and policies, primarily in the area of foreign, security, and defence policies, including the collective response under Article 42 para. 7 TEU (mutual assistance) and Article 222 TFEU (obligation of solidarity). Such measures should be decided on a case-by-case basis; comply with both the international law and the EU's strategic interests; and ultimately be well-calibrated and proportionate to the scope, scale, duration, intensity, complexity, sophistication, and impact of each hybrid campaign. It requires optimal situational awareness, often lacking in cases of a concerted hybrid threat or campaign. A coordinated response at the EU level can be instigated against malicious hybrid activities that constitute internationally wrongful acts and against those that are merely considered unfriendly acts. The attribution of responsibility for hybrid activities to a particular state or non-state actor is not a precondition for the implementation of countermeasures at the EU level; nevertheless, some measures (e.g. sanctions) can only be targeted. Compared

to the international legal framework, the framework of the EU (compared to NATO) "theoretically" offers wider possibilities for a collective response to hybrid threats and campaigns by enabling the invocation of the mutual solidarity clause (Article 222 TFEU) in situations that otherwise could not trigger the collective defence mechanism under Article 5 NATO Treaty. Nevertheless, the possible application of Article 222 TFEU or Article 42 para. 7 TEU (mutual defence clause) to hybrid attacks has not yet been assessed or implemented in practice.

The analysis in this chapter demonstrates that it is hardly possible to generally and unequivocally conclude whether the use of hybrid threats and warfare leads to *de facto* combat that amounts to the use of force, and whether it triggers legal consequences attached to the existence of armed conflict, especially if the hybrid campaign does not involve the use of kinetic force. Balancing between war and peace, hybrid warfare could indeed substitute for Schrödinger's cat. It aptly highlights how the international community and international legal order thrives on the traditional dichotomy between war and peace – a dichotomy that is hardly compatible with the realities of international relations and works in favour of hybrid aggressors.[188] Facilitating the application of existing international standards to hybrid threats and warfare through a clearer interpretation of the relevant thresholds and legal consequences would amount to effective "lawmunition", translating into better preparedness and resilience. However, in the author's opinion, any interpretation or re-interpretation of the existing international standards, albeit necessary, should be guided by the spirit of the UN Charter, which seeks to protect our children and grandchildren from the scourge of war.[189]

188 George F. Kennan, 1948, para. 1, expressed that concern already in 1948:
We have been handicapped however by a popular attachment to the concept of a basic difference between peace and war, by a tendency to view war as a sort of sporting context outside of all political context, by a national tendency to seek for a political cure-all, and by a reluctance to recognize the realities of international relations – the perpetual rhythm of struggle, in and out of war.

189 Teleological interpretation is an imperative that stems from the interpretation guidelines contained in Article 31 para. 1 of the *Vienna Convention on the Law of Treaties*, adopted in Vienna on 23 May 1969, UN Treaty Series vol. 1155, Reg. no. 18232.

References

Arthur, J.E. (2020) 'Russian Cyber Campaigns in Support of Military Operations', *American Intelligence Journal*, 37(1), pp. 49–53.

Aukia, J., Kubica, L. (2023) 'Russia and China as hybrid threat actors: The shared self-other dynamics', *Hybrid CoE Research Reports*, *The European Centre of Excellence for Countering Hybrid Threats*, March 2023. [Online]. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/NEW_Hybrid_CoE_Research_Report_8_web.pdf (Accessed: 31 January 2024).

Bakker, A., Biscop, S., Drent, M., Landman, L. (2016) *Spearheading European Defence. Employing the Lisbon Treaty for a Stronger CSDP.* The Hague: Netherlands Institute of International Relations Clingendael.

Bekić, J. (2022) 'Coercive Engineered Migrations as a Tool of Hybrid Warfare', *Croatian Political Science Review*, 59(2), pp. 141–169; https://doi.org/10.20901/pm.59.2.06.

Bendiek, A., Schulze, M. (2021) *Attribution – a Major Challenge for EU Cyber Actions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW.* Berlin: German Institute for International and Security Affairs; https://doi.org/10.18449/2021RP11.

Bingle, M. (2023) 'What is Information Warfare?', *The Henry M. Jackson School of International Studies, University of Washington*, 25 September 2023. [Online]. Available at: https://jsis.washington.edu/news/what-is-information-warfare (Accessed: 31 January 2024).

Blake-Martin, D. (2023) 'Interview – Kelly Greenhill', *E-International Relations*, 5 February 2023. [Online]. Available at: https://www.e-ir.info/2023/02/05/interview-kelly-greenhill (Accessed: 31 January 2024).

van den Bosch, B. (2021) 'Fighting a war without violence. The rules of International Humanitarian Law for military cyber-operations below the threshold of 'attack'' in Johnson, R., Kitzen, M., Sweijs, T. (eds.) *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic*. London: Routledge, pp. 211–222; https://doi.org/10.4324/9781003054269-19.

CAHDI (2018) 'Opinion of the CAHDI: On Recommendation 2130 (2018) of the Parliamentary Assembly of the Council of Europe – "Legal Challenges Related to Hybrid War and Human Rights Obligations"', *Council of Europe*, 2018. [Online]. Available at: https://rm.coe.int/opinion-of-the-cahdi-on-recommendation-2130-2018-of-the-parliamentary-/1680907884 (Accessed: 31 January 2024).

Cassese, A. (2008) 'Current Trends in the Development of the Law of Armed Conflict' in Gaeta, P., Zappalà, S. (eds.) *The Human Dimension of International Law: Selected Papers*. New York: Oxford Academic Press, pp. 4–38; https://doi.org/10.1093/acprof:oso/9780199232918.003.0001.

Clarke, M. (2019) 'China's Application of the 'Three Warfares' in the South China Sea and Xinjiang', *Orbis*, 63(2), pp. 187–208; https://doi.org/10.1016/j.orbis.2019.02.007.

Cochran, E.S. (2020) 'China's "Three Warfares": People's Liberation Army Influence Operations', *International Bulletin of Political Psychology*, 20(3), pp. 1–24.

Committee on Legal Affairs and Human Rights (2018) 'Legal Challenges Related to Hybrid War and Human Rights Obligations', *Parliamentary Assembly of the Council of Europe*, 6 April. [Online]. Available at: https://pace.coe.int/en/files/24547 (Accessed: 31 January 2024).

Council of Europe (2022) 'Legal Analysis of the Derogation Made by Ukraine under Article 15 of the European Convention of Human Rights and Article 4 of the International Covenant on Civil and Political Rights', *Council of Europe*, November 2022. [Online]. Available at: https://rm.coe.int/legal-analysis-of-the-derogation-made-by-ukraine-under-article-15-of-t/1680aa8e2c (Accessed: 31 January 2024).

Council of the EU (2021a) 'Belarus: EU Adopts 5th Package of Sanctions Over Continued Human Rights Abuses and the Instrumentalisation of Migrants', *Council of the EU and the European Council*, 2 December. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/12/02/belarus-eu-adopts-5th-package-of-sanctions-over-continued-human-rights-abuses-and-the-instrumentalisation-of-migrants/ (Accessed: 31 January 2024).

Council of the EU (2021b) 'Belarus: EU Broadens Scope for Sanctions to Tackle Hybrid Attacks and Instrumentalisation of Migrants', *Council of the EU and the European Council*, 15 November. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/11/15/belarus-eu-broadens-scope-for-sanctions-to-tackle-hybrid-attacks-and-instrumentalisation-of-migrants/ (Accessed: 31 January 2024).

Deen, B., Zandee, D., Stoetman, A. (2022) *Uncharted and uncomfortable in European defence. The EU's mutual assistance clause of Article 42(7).* The Hague: Netherlands Institute of International Relations Clingendael.

Dinstein, Y. (2011) *War, aggression, and self-defence*. 5th edn. Cambridge: Cambridge University Press; https://doi.org/10.1017/CBO9780511920622.

Dörr, O., Randelzhofer, A. (2015) 'Article 2(4)' in Simma, B., Khan D.-E., Nolte, G., Paulus A., Wessendorf, N. (eds.) *The Charter of the United Nations: A Commentary, Volume I*. 3rd edn. Oxford: Oxford University Press.

Dunlap, C.J. (2001) 'Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts' presented at *Humanitarian Challenges in Military Interventions Conference* (29 November 2001). [Online]. Available at: https://scholarship.law.duke.edu/faculty_scholarship/3500/ (Accessed: 31 January 2024).

Dunlap, C.J. (2008) 'Lawfare Today: A Perspective', *Yale Journal of International Affairs*, Winter 2008, pp. 146–154.

Erlbacher, F. (2019) 'Article 222' in Kellerbauer, M., Klamert, M., Tomkin, J. (eds.) *The EU Treaties and the Charter of Fundamental Rights. A Commentary.* 1st edn. Oxford: Oxford University Press, pp. 1690–1696.

European Commission (2021a) '2021 State of the Union Address by President von der Leyen', *European Commission*, 15 September. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701 (Accessed: 31 January 2024).

European Commission (2021b) 'Von der Leyen on Belarus: The EU Has the Will, the Unity and the Resolve to Face This Crisis', *European Commission*, 23 November. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/AC_21_6254 (Accessed: 31 January 2024).

European Council (2014) 'Statement of the Heads of State or Government on Ukraine', *Council of the EU and the European Council*, 6 March. [Online]. Available at: https://www.consilium.europa.eu/media/29285/141372.pdf (Accessed: 31 January 2024).

European Council (2021) 'Remarks by President Charles Michel After His Meeting with the Prime Minister of Poland, Mateusz Morawiecki, in Warsaw' *Council of the EU and the European Council*, 10 November. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/11/10/intervention-du-president-charles-michel-a-l-issue-de-sa-rencontre-avec-le-premier-ministre-polonais-mateusz-morawiecki-a-varsovie (Accessed: 31 January 2024).

Federation Council of the Federal Assembly of the Russian Federation (2019) 'Statement of the Federation Council of the Federal Assembly of the Russian Federation', *Federation Council*, 10 April. [Online]. Available at: http://council.gov.ru/en/activity/docs/en/104357/ (Accessed: 31 January 2024).

Fogt, M.M. (2020) 'Legal Challenges or 'Gaps' by Countering Hybrid Warfare: Building Resilience in Jus ante Bellum', *Southwestern Journal of International Law*, 27(1), pp. 28–100.

Franke, U. (2015) *War by non-military means. Understanding Russian information warfare*, Stockholm: Försvarsdepartementet.

Giannopoulos, G., Smith, H., Theocharidou, M. (2021) *The Landscape of Hybrid Threats: A conceptual model*. Luxembourg: Publications Office of the European Union; https://doi.org/10.2760/44985.

Greenhill, K.M. (2010) 'Weapons of Mass Migration: Forced Displacement as an Instrument of Coercion', *Strategic Insights*, 9(1), pp. 116–160.

Greenwood, C. (1987) 'The concept of war in modern international law', *International and Comparative Law Quarterly*, 36(2), pp. 283–306.

Hathaway, O.A. (2014) 'Fighting The Last War: The United Nations Charter In The Age Of The War On Terror' in Shapiro, I., Lampert, J. (eds.) *Charter of the United Nations: Together with Scholarly Commentaries and Essential Historical Documents*. New Haven: Yale University Press, pp. 210–224; https://doi.org/10.12987/9780300182538-011.

Heap, B. (ed.) (2021) *Strategic Communications Hybrid Threats Toolkit. Applying the principles of NATO Strategic Communications to understand and counter grey zone threats*. Riga: NATO Strategic Communications Centre of Excellence.

Hoffman, F.G. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.

Huttunen, J. (2024) 'Countering Instrumentalised Migration: The case for Border Closure Through a Derogation under the ECHR', *EJIL:Talk! Blog of the European Journal of International Law*, 2 January 2024. [Online]. Available at: https://www.ejiltalk.org/countering-instrumentalised-migration-the-case-for-border-closure-through-a-derogation-under-the-echr/ (Accessed: 31 January 2024).

International Committee of the Red Cross (2004) *What is International Humanitarian Law. Legal factsheet.* [Online]. Available at: https://www.icrc.org/en/download/file/240610/what_is_ihl.pdf (Accessed: 31 January 2024).

International Committee of the Red Cross (2016) *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. 2nd edn. Cambridge: Cambridge University Press. [Online]. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-2/commentary/2016 (Accessed: 31 January 2024).

Ionita, C.-C. (2023) 'Conventional and hybrid actions in the Russia's invasion of Ukraine', *Security and Defence Quarterly*, 44(4), pp. 5–20; https://doi.org/10.35467/sdq/168870.

Johnson, R. (2021) 'Hybrid Warfare and Counter-Coercion' in Johnson, R., Kitzen, M., Sweijs, T. (eds.) *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic*. London: Routledge, pp. 45–57; https://doi.org/10.4324/9781003054269-5.

Johnson, D. (2015) 'Russia's Approach to Conflict – Implications for NATO's Deterrence and Defence', *Research Division-NATO Defense College Rome*, 2015/111, pp. 1–12.
Jordan, T.P. (2016) 'The Law of Armed Conflict, Unconventional Warfare, and Cyber Attacks', *American University National Security Law Brief*, 6(2), pp. 37–58.
Kania, E. (2016) 'The PLA's Latest Strategic Thinking on the Three Warfares', *China Brief Volume*, 16(13). [Online]. Available at: https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/ (Accessed: 31 January 2024).
Karski, K., Mielniczek, P. (2019) 'The notion of hybrid warfare in international law and its importance for NATO', *NATO Legal Gazette,* 2019/39, pp. 67–80.
Kennan, G.F. (1948) '269. Policy Planning Staff Memorandum', *Office of the Historian*, 4 May 1948. [Online]. Available at: https://history.state.gov/historicaldocuments/frus1945-50Intel/d269 (Accessed: 31 January 2024).
Kittrie, O.F. (2016) *Lawfare: Law as a Weapon of War.* Oxford: Oxford University Press; https://doi.org/10.1093/acprof:oso/9780190263577.001.0001.
Kowalczewska, K. (2014) 'Lawfare: inter arma… leges arma?', *Międzynarodowe Prawo Humanitarne*, 2014/5, pp. 38–53.
The Kremlin, Moscow (2014) 'Address by President of the Russian Federation', *President of Russia*, 18 March. [Online]. Available at: http://en.kremlin.ru/events/president/news/20603 (Accessed: 31 January 2024).
Lasconjarias, G., Larsen, J.A. (eds.) (2015) *NATO'S Response to Hybrid Threats*. 1st edn. Rome: NATO Defense College.
Lauterpacht, H. (1952) 'The problem of the revision of the law of war', *British Yearbook of International Law*, 1952/29, pp. 360–382.
Lauterpacht, E. (1968) 'The Legal Irrelevance of the State of War', *American Society of International Law Proceedings*, 1968/62, pp. 58–67; https://doi.org/10.1017/S0272503700014919.
Lesaffer, R. (2015) 'Too Much History: From War as Sanction to the Sanctioning of War' in Weller, M. (ed.) *The Oxford Handbook of the Use of Force in International Law.* 1st edn. Oxford: Oxford University Press, pp. 35–55; https://doi.org/10.1093/law/9780199673049.003.0002.
Lott, A. (2022) *Hybrid Threats and the Law of the Sea. Use of Force and Discriminatory Navigational Restrictions in Straits*. 1st edn. Leiden: Brill-Nijhof, pp. 16–36; https://doi.org/10.1163/9789004509368_004.
Łubiński, P. (2021) 'Hybrid Warfare or Hybrid Threat – The Weaponization of Migration as an Example of the Use of Lawfare – Case Study of Poland', *Polish Political Science Yearbook*, 2021/51, pp. 1–13; https://doi.org/10.15804/ppsy202209.
Medina Llinàs, M. (2022) 'Hybrid attacks on critical infrastructure' in Bargués, P., Bourekba, M., Colomina, C. (eds.) *Hybrid threats, vulnerable order.* Barcelona: Barcelona Centre for International Affairs.
Mik, C. (2022) 'Russia's Aggression against Ukraine: a Clash of Two Visions of the International Community and International Law', *Polish Review of International and European Law*, 12(2), pp. 57–113; https://doi.org/10.21697/2022.12.2.5.
Martin, M. (2021) 'China's Three Information Warfares', *Proceedings*, vol. 147/3/1,417, March 2021. [Online]. Available at: https://www.usni.org/magazines/proceedings/2021/march/chinas-three-information-warfares (Accessed: 31 January 2024).

Mansoor, P.R. (2012) 'Hybrid Warfare in History' in Murray, W., Mansoor, P.R. (eds.) *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. New York: Cambridge University Press.

Mauer, P. (2023) 'Strategies for Reconciling International Humanitarian Law and Cyber Operations: A Q&A with Dr. Peter Maurer', *Digital Front Lines*. [Online]. Available at: https://digitalfrontlines.io/2023/07/11/strategies-for-reconciling-international-humanitarian-law-and-cyber-operations/ (Accessed: 31 January 2024).

Moussa, J. (2008) 'Can jus ad bellum override jus in bello? Reaffirming the separation of the two bodies of law', *International Review of the Red Cross*, 90(872), pp. 963–990; https://doi.org/10.1017/S181638310900023X.

Munoz Mosquera, A.B., Bachmann, S.D. (2015) 'Lawfare and hybrid warfare – how Russia is using the law as a weapon', *Amicus Curiae*, 2015/102, pp. 25–28; https://doi.org/10.14296/ac.v2015i102.2433.

Munoz Mosquera, A.B., Bachmann, S.D. (2016) 'Lawfare in Hybrid Wars: The 21st Century Warfare', *Journal of International Humanitarian Legal Studies*, 7(1), pp. 63–87; https://doi.org/10.1163/18781527-00701008.

NATO (2013) *Allied Command Operations Comprehensive Operations Planning Directive Interim Version 2.0 (COPD V 2.0)*. Brussels: NATO Unclassified.

NATO (2015) 'Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar', *NATO*, 25 March. [Online] Available at: https://www.nato.int/cps/en/natohq/opinions_118435.htm (Accessed: 31 January 2024).

NATO (2016) 'Warsaw Summit Communiqué', *NATO*, 9 July. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Accessed: 31 January 2024).

NATO (2022) 'NATO 2022 Strategic Concept: Adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022', *NATO*, 29 June. [Online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (Accessed: 31 January 2024).

Najžer, B. (2020) *The Hybrid Age: International Security in the Era of Hybrid Warfare*. 1st edn. London: I. B. Tauris; https://doi.org/10.5040/9780755602544.

Nagy, Z., Horváth, A. (eds.) (2022) *Emergency Powers in Central and Eastern Europe: From Martial Law to COVID-19*. 1st edn. Budapest-Miskolc: Ferenc Mádl Institute of Comparative Law, Central European Academic Publishing; https://doi.org/10.47079/2022.znah.epicaee.1.

Nováky, N.I.M. (2017) 'The Invocation of the European Union's Mutual Assistance Clause: A Call for Enforced Solidarity', *European Foreign Affairs Review*, 22(3), pp. 357–375; https://doi.org/10.54648/eerr2017030.

Parulski, K. (2016) 'Legal Aspects of Hybrid Warfare in Ukraine', *Zeszyty Naukowe AON*, 4 (105), pp. 5–27.

President of Russia (2014) 'Direct Line with Vladimir Putin', *President of Russia*, 17 April 2014. [Online]. Available at: http://en.kremlin.ru/events/president/news/20796 (Accessed: 31 January 2024).

Ramopoulos, T. (2019) 'Article 42 TEU' in Kellerbauer, M., Klamert, M., Tomkin, J. (eds.) *The EU Treaties and the Charter of Fundamental Rights. A Commentary*. 1st edn. Oxford: Oxford University Press, pp. 277–282.

Sanz Caballero, S. (2023) 'The concepts and laws applicable to hybrid threats, with a special focus on Europe', *Humanities and Social Sciences Communications*, 2023/10, pp. 1–8; https://doi.org/10.1057/s41599-023-01864-y.

Sari, A. (2017) 'Hybrid Warfare, Law and the Fulda Gap', *University of Exeter – Law School*. [Online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927773 (Accessed: 31 January 2024).

Sari, A. (2023) 'Instrumentalized migration and the Belarus crisis: Strategies of legal coercion', *Hybrid CoE Paper No. 17, The European Centre of Excellence for Countering Hybrid Threats*, April 2023. [Online]. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230425-Hybrid-CoE-Paper-17-Instrumentalized-migration-and-Belarus-WEB.pdf (Accessed: 31 January 2024).

Schabas, W.A. (2015) *The European Convention on Human Rights. A Commentary*. 1st edn. New York: Oxford University Press; https://doi.org/10.1093/law/9780199594061.001.0001.

Schmitt, M.N. (2015) 'The Use of Cyber Force and International Law' in Weller, M. (ed.) *The Oxford Handbook of the Use of Force in International Law*. 1st edn. Oxford: Oxford University Press, pp. 1110–1130; https://doi.org/10.1093/law/9780199673049.003.0053.

Secretariat General (2015) 'JJ7979C Tr./005-185', *Council of Europe*, 10 June. [Online]. Available at: https://rm.coe.int/09000016804896cf (Accessed: 31 January 2024).

Secretariat General (2022) 'JJ9325C Corrigendum Tr./005-287', *Council of Europe*, 2 March. [Online]. Available at: https://rm.coe.int/1680a5b0b0 (Accessed: 31 January 2024).

Soldatenko, M. (2023) 'Constructive Ambiguity of the Budapest Memorandum at 28: Making Sense of the Controversial Agreement', *Lawfare Foreign Relations & International Law*, 7 February 2023. [Online]. Available at: https://www.lawfaremedia.org/article/constructive-ambiguity-of-the-budapest-memorandum-at-28-making-sense-of-the-controversial-agreement (Accessed: 31 January 2024).

Sun Tzu (2010) *The Art of War: timeless military strategy from 6th Century China* (transl. Lionel Giles). Rookhope: Aziloth Books.

Tallis, B., Šimečka, M. (2017) *Collective Defence in the Age of Hybrid Warfare*. Prague: Institute of International Relations. [Online]. Available at: https://www.iir.cz/priloha?page=collective-defence-in-the-age-of-hybrid-warfare&p=1&type=news_cs (Accessed: 31 January 2024).

Veress, C. (2023) 'Kisebbségi jogok felhasználása hibrid hadviselési eszközként' [Using minority rights as a hybrid warfare tool], *Nemzetközi tevékenység*, 2023/1, pp. 29–40; https://doi.org/10.35926/HSZ.2023.1.3.

Voyger, M. (2015) 'Russia's Use of 'Legal' as an Element of its Comprehensive Warfare Strategy', *LandPower Magazine*, 1(2), p. 20.

Wentzell, T.D. (2021) 'Russia's Green Men: The Strategic Storytellers of Hybrid Warfare', *Canadian Military Journal*, 22(1), pp. 42–48.

Wyrozumska, A. (2014) 'The Opinion by the Legal Advisory Committee to the Minister of Foreign Affairs of the Republic of Poland on the Annexation of the Crimean Peninsula to the Russian Federation in Light of International Law', *Polish Yearbook of International Law*, 2014/34, pp. 275–278; https://doi.org/10.7420/pyil2014l.

Yablokov, I. (2022) 'Russian disinformation finds fertile ground in the West', *Nature Human Behaviour*, vol. 6, pp. 766–767; https://doi.org/10.1038/s41562-022-01399-3.

Statement of the Prime Ministers of Poland, Lithuania, Latvia and Estonia on the hybrid attack on our borders by Belarus (2021) gov.pl, 23 August 2021. [Online]. Available at: https://www.gov.pl/web/nato-en/statement-of-the-prime-ministers-of-poland-lithuania-latvia-and-estonia-on-the-hybrid-attack-on-our-borders-by-belarus (Accessed: 31 January 2024).

Part V

CRITICAL INFRASTRUCTURE PROTECTION

Chapter 18

Selected Legal Aspects of National Security and Critical Infrastructure Protection in the European Union with Particular Reference to the Polish National Legislation

Grzegorz Ocieczek

Abstract

In the current geopolitical scenario, ensuring national security and the protection of critical infrastructure seem to be key elements for upholding the proper functioning of a state and, consequently, the safety of its citizens. This paper addresses issues related to the protection of critical infrastructure in territory of the European Union (EU). Particular attention is paid to issues regarding legal solutions to ensure the security of EU member states. EU directives concerning the immunity of critical entities (CER) and issues related to ensuring a high level of cybersecurity in the territory of the EU (NIS 2) are discussed. The paper is divided into several main parts, which, in addition to the above-mentioned issues regarding the legal aspects of critical infrastructure protection, also address security (e.g. types and divisions) and terrorism (e.g. the most important legal acts aimed at counteracting this very dangerous phenomenon is indicated). This study also discusses the European Security Strategy (2020–2025) and its most important objectives regarding the security of critical infrastructure, anti-terrorism, cybersecurity, and the protection of public spaces. Regarding national security, the paper discusses the various national security strategies from 1990 to the present in Poland, showing that the strategies pay

Grzegorz Ocieczek (2024) 'Selected Legal Aspects of National Security and Critical Infrastructure Protection in the European Union with Particular Reference to the Polish National Legislation'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 803–839. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_18

particular attention to the changing approaches to security, the assessment of the current situation at the time and threats involved, and the increasing need to ensure the protection of critical infrastructure. The publication ends with conclusions and postulates regarding the need to ensure national security and increase the protection of critical infrastructure.

Keywords: Critical infrastructure, national security, terrorism, cybersecurity, national security strategies, European security strategies.

---

1. Introduction: critical infrastructure

1.1. Concept and division of hazards

Directly related to the issue of security is the so-called negative definition of security or threat is directly related to security issues. According to the definition of the term "threat" in the Polish dictionary, 'a "threat" is a situation or condition that threatens someone or in which he or she feels threatened as well as someone who creates such a situation'.[1] According to Professor Kitler, a threat is defined as 'a state of mental consciousness caused by phenomena perceived as negative (dangerous), and at the same time it is a set of internal and (or) external circumstances that can cause a dangerous state for a given subject'.[2] In turn, Ficoń defined danger as: 'an event caused by fortuitous (natural) or non-fortuitous (intentional) causes, which has a negative impact on the functioning of a given system or causes adverse (dangerous) changes in its structure or functioning'.[3] Most authors propose what is known as the dichotomous division of hazards, namely, those caused independently of humans and those caused by humans.[4]

Certainly, the development of different categories of hazards is favoured by the development of civilisation, which can be considered an accelerator of phenomena that can be categorised as dangerous. With regard to the division of hazards, the following criteria for their emergence should be distinguished: the possibility of anticipation (e.g. controlled, forecastable, unpredictable); source of origin (e.g. natural, technical, social, civilisational, and/or environmental); type (e.g. small, medium, large); elimination time (e.g. short-, medium-, and long-term); causal determinism

1 *Słownik Języka Polskiego PWN* [Dictionary of the Polish Language PWN], word: "security". [Online]. Available at: https://sjp.pwn.pl/slowniki/bezpieczeństwo (Accessed: 21 August 2022).
2 Kitler, 2010, p. 52.
3 Ficoń, 2007, p. 76.
4 See, for example: Glen, 2011, p. 19 et seq.

(e.g. intentional, random, mixed). Another division of hazards is also proposed herein: spatial coverage (e.g. local, regional, national, international, and global); field of action (e.g. sectoral, religious, political, and universal); level of destruction (e.g. minimal, medium, and high total).[5]

Meanwhile, nonmilitary threats can take the form of natural hazards (e.g. natural disasters), risks associated with human activities (e.g. pollution, activities, ozone holes, and environmental predation), and risks of an extraordinary nature (e.g. accidents, disasters, riots, disruptions of all kinds in transport and energy).[6] Another typology of risks is as follows: (1) natural hazards (e.g. droughts, frosts, floods, fires, winds, earthquakes, avalanches, and precipitation); (2) military threats (e.g. by type of formation, by means of destruction); (3) social risks (e.g. social pathologies and mental disorders); (4) technical hazards (e.g. environmental, communication, technological, construction, municipal, and network emergencies).[7]

1.2. Critical infrastructure worldwide: focusing on the European Union

The concept of critical infrastructure describes that certain resources essential for the functioning of the state, as they provides services of strategic importance and, above all, necessary for daily life in the form of communication, transportation, energy, water, and health. Therefore, the destruction or damage to critical infrastructure can have irreversible consequences not only for the residents of the country in which the incident occurred but also for residents of neighbouring countries. The malfunction of critical infrastructure can additionally cause negative social and economic consequences.

Turning to the question of critical infrastructure, and in particular the need to protect it and ensure the security of the population living in a given territory, in ancient times critical infrastructure played a significant role in the functioning of the state. Examples include the irrigation facilities on the Nile, the grain storage facilities or the ports of Phoenicia, and the aqueducts in Rome. The proper functioning of critical infrastructure increases citizen security and the state of certainty. With regard to the protection of critical infrastructure, it becomes impossible not to mention the events in the world that have increased public awareness of this issue, and thus have been accelerators of actions to ensure its proper protection and security. On 13 and 14 July 1977, a power line failure in New York City left the city without electricity for two days. This event was followed by riots which resulted in the looting and destruction of 1,616 shops.[8] In addition to the aforementioned accidents, there is the major accident at the Fukushima nuclear power plant, which occurred as a result of the tsunami caused by the earthquake on 11 March 2011, off the

5 Ficoń, 2007, p. 78.
6 Mierzejewski, 2011, p. 48.
7 Jakubczak, 2008, p. 402.
8 Wadowski, 2018, p. 1237.

coast of Honshu Island. These events have resulted in an estimated 15.000–20.000 deaths.[9] The accident had a greater impact than the Chernobyl reactor accident on 26 April 1986, which was caused by operator errors.[10]

Mention should also be made of the massive attack on Estonia's critical infrastructure on 27 April 2007, when hackers affiliated with the Russian Federation are believed to have launched a massive attack that paralysed the country. After that evening, the wave of cyberattacks on the information technology (IT) infrastructure of the country only escalated, as the websites of the parliament, defence and justice ministries, political parties, the police, and even public schools were disabled. The cyberwar lasted for three weeks. During that time, after the initial surprise, a quickly-formed unit (Estonian Computer Emergency Response Team, also known as CERT-EE), led by Hillar Aarelaid, organized an improvised but ultimately effective defence until May 18, when the attacks abruptly stopped.[11] The most recent attacks on critical infrastructure took place in early March 2024 when the Asia-Africa-Europe 1, Europe India Gateway, Seacom, and TGN-Gulf cable networks were damaged. These attacks significantly hampered the passage through and around the Red Sea. The area has accounts for approximately 12% of maritime trade worldwide in recent years, and yet some ships are opting for longer circuitous routes because of the fear of repercussions.[12]

The first documents describing critical infrastructure protection issues were the 'Protocol Additional I to the Geneva Conventions of 12 August 1949', and the 'Protocol Additional II to the Geneva Conventions of 12 August 1949'. For example, Art. 55 of the Protocol Additional I deals with the protection of the environment, while its Art. 56 deals with the protection of structures and installations containing dangerous forces. According to para. 1 of Art. 56, structures and installations containing dangerous forces, particularly dams, dykes, and nuclear power stations, may not be subjected to attacks, even if they are military targets, as such attacks are likely to trigger such forces and consequently cause serious harm to the civilian population. Other military targets on or near such structures or facilities should not be subjected to attacks, as they are likely to trigger dangerous forces and consequently cause serious civilian casualties.[13]

In 1998, Bill Clinton issued a directive (named PDD-63) on critical infrastructure protection, the aim of which was to increase protection against possible terrorist attacks as well as the security of critical infrastructures. According to this document, critical infrastructure encompasses both physical and cyber-based system essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation,

9 Jędrak, 2022; Wiech, 2021.
10 *Katastrofa w Czarnobylu* [Chernobyl disaster], no date.
11 Jalonen, 2009.
12 *Incydent na Morzu Czerwonym. Kluczowe kable przecięte* [Incident on the Red Sea. Key cables cut], 2024.
13 Art. 56(1) of the Protocol Additional to the Geneva Conventions of 12 August 1949.

water systems and emergency services, both governmental and private. Importantly, it was ordered that the state sector cooperate with the private sector to protect such critical infrastructure. According to the US Department of Homeland Security, approximately 85% of critical infrastructure remains in the private sector.[14] Immediately prior to this directive, on 15 July 1996, Executive Order 13010 was issued, based on which the President's Commission on Critical Infrastructure Protection was established. This Order also includes the definition of critical infrastructure, as follows:

> a structure of interdependent networks and systems comprising, identifiable industries, institutions (including people and procedures), and distribution capabilities that provide the flow of products and services essential to the defence and economic security of the United States, the smooth functioning of government at all levels, and society as a whole.[15]

In the immediate aftermath of the terrorist attack on 11 September 2001, 27 pieces of legislation were enacted in the United States to intensify the protection of critical infrastructure.[16] One of the most important pieces was the Homeland Security Presidential Directive No. 7 of 17 December 2003, concerning the identification, priority, and protection of critical infrastructure of the state.[17]

Another important international document was the Council Directive of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection.[18] This Directive followed the adoption, on 20 October 2004, of Communication from the Commission on a European programme for critical infrastructure protection,[19] proposing ways to improve Europe's prevention of, preparedness for, and response to terrorist attacks against critical infrastructure. There was also the adoption of the Green Paper on a European Programme for Critical Infrastructure Protection (also known as EPCIP), which provided policy options for the development of the Programme and the Critical Infrastructure Warning Information Network. Art. 2a of the Directive defines critical infrastructure as a component, system, or part thereof, located in European Union (EU) Member States which is essential for the maintenance of vital societal functions, health, safety, security, material, or social well-being, and which

14 Szewczyk and Pyznar, 2010, p. 53.
15 Heniff, 2004, p. 5.
16 Radvanovsky and McDougall, 2010, pp. 289–293.
17 Tyburska, 2011, p. 147.
18 *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. The previous document was: *The Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, of 12 December 2006*.
19 *Green Paper on a European programme for critical infrastructure protection,* Para. 1, p. 2. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576 (Accessed: 21 August 2023).

would have a significant impact on a Member State in case disrupted or destroyed as a result of the loss of these functions. Art. 2b, in turn, defines the concept of European Critical Infrastructure (described as ECI), which refers to critical infrastructures located within the territory of Member States, the disruption or destruction of which would significantly affect two or more Member States. Whether the impact is significant is assessed with reference to crosscutting criteria, including impacts resulting from cross-sectoral interdependencies with other infrastructure.[20] The Directive also includes relevant considerations such as recognition of ECI, designation of ECI, protection plans, security liaison officers, and sensitive critical infrastructure protection information.

According to Annex 1 of the above Directive, the basic sectors to which critical infrastructure should be designated are the energy sector (e.g. electricity, oil, and gas) and the transport sector (e.g. road, rail, air, inland waterway, ocean shipping, short sea shipping, and ports).[21] Particularly important documents that have been published recently as part of the so-called Critical Infrastructure Protection regulatory package, which represents the latest developments on the issue, are as follows:

1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011;[22]
2. Directive on measures for a high common level of cybersecurity across the Union (NIS2) of 14 December 2022;[23]
3. Directive amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366, and (EU) 2016/2341 as regards digital operational resilience for the financial sector;[24]
4. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.[25]

20 Arts. 2a and 2b of *the Council Directive 2008/114/EC of 8 December 2008, on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*.

21 *Annex No. 1, Council Directive 2008/114/EC of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*.

22 *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*.

23 *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148* (NIS 2 Directive).

24 *Document 32022L2556, Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022, amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (Text with EEA relevance), PE/42/2022/REV/1*.

25 *Critical Entity Resilience (CER) Directive of 27 December 2022*.

The implementation of the aforementioned legislation was primarily linked to the need for effective cyber security preparedness, as well as the range of risks emanating from it. Additionally, the COVID-19 pandemic and its negative impacts highlighted the need for a seamless supply chain.

The first piece of legislation, the Regulation of the European Parliament and of the Council (EU) on digital operational resilience for the financial sector, highlights issues related to information and communication technologies (ICTs) that support the complex systems used in day-to-day operations. According to point 1 of the Regulation,

> ICT keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectedness also amplify ICT risk, making society as a whole and the financial system more vulnerable to cyber threats or ICT disruptions.

This explains why the importance of the need to increase digital resilience, the definition of resilience standards, and the coordination of regulatory and supervisory work in this area. Another piece of legislation, the Directive on measures for a high common level of cyber-security within the Union (NIS2), calls in its sixth point for the extension of the scope of the rules by sector to the wider economy, so as to ensure that sectors and services essential for key social and economic activities in the internal market are comprehensively covered. In particular, this Directive seeks to address the shortcomings of the distinction between key service operators and digital service providers, as it has proven outdated by not reflecting the importance of the sectors or services concerned with social and economic activities in the internal market. In addition, the Directive sets a benchmark for cybersecurity risk management measures and incident reporting obligations in the sectors within its scope. Point 19 of the Directive further mentions that:

> Member States should be responsible for submitting to the Commission at least the number of essential and important entities for each sector and subsector referred to in the annexes, as well as relevant information about the number of identified entities and the provision, from among those laid down in this Directive, on the basis of which they were identified, and the type of service that they provide.

Regarding the issue of possible incidents, 'Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate incidents and risks' (point 41 of the Directive). Mutual international cooperation and coordination in preventing and restoring critical infrastructure and, most importantly, proper risk management are also important.

The Critical Entities Resilience Directive (CER) of 14 December 2022 repealing Council Directive 2008/114/EC, states in its first point that,

> Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market in an increasingly interdependent Union economy. It is therefore essential to set out a Union framework with the aim of both enhancing the resilience of critical entities in the internal market by laying down harmonised minimum rules and assisting them by means of coherent and dedicated support and supervision measures.

An important indication is provided by the recommendations described in point 43, according to which:

> As the objectives of this Directive cannot be sufficiently achieved by the Member States since they require harmonisation of requirements already contained in Directives. By reason of the scale and effects of the action, they can be better achieved at Union level. Action may be taken in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

The Directive amending Directives 2009/65/EC, et al. with regard to the operational digital resilience of the financial sector signals in its first point that:

> The Union needs to adequately and comprehensively address digital risks to all financial entities stemming from an increased use of information and communication technology (ICT) in the provision and consumption of financial services, thereby contributing to the realisation of the potential of digital finance, in terms of boosting innovation and promoting competition in a secure digital environment.

In accordance with Directive 2022/2557, there is no reduction in national laws, and the country can provide a higher level of resilience to critical actors. In addition, a strategy should be developed within 36 months to enhance the resilience of critical entities, and it is recommended that the Directive be updated every four years. Furthermore, it is important for EU Member States to conduct risk assessment, and the States have 36 months to identify critical entities. It is also important to indicate the criteria for determining the significance of the disruptive effect. Each country shall designate at least one authority responsible for national implementation and enforcement of the provisions set forth in this Directive. At the same time, EU Member States are required to support critical entities in enhancing their resilience through guidelines, methodologies, exercises, and training. In this regard, good cooperation among EU Member States in protecting critical infrastructure is necessary (Art. 7 of Directive 2022/2527). Under this Directive, critical entities must implement appropriate and proportionate technical, security, and organisational measures to ensure resilience. Critical entities, according to the relevant regulations, are given a tool to check the background of critical personnel in EU registries. In addition, the

European Commission may organise an advisory mission to assess the measures put in place by a critical entity to fulfil its obligations. Simultaneously, EU Member States shall ensure that European critical entities provide advisory missions with access to information, systems, and facilities related to the provision of critical services, as these necessary for the work of the advisory mission. Another important aspect is that EU Member States shall ensure that competent authorities have the power and means to carry out on-site inspections of the critical infrastructure, buildings, and premises used by the critical entity to provide critical services, and remotely monitor the critical entity's measures, as well as conduct or commission audits of critical entities.

According to this all-important Directive, the critical entity should provide evidence of effective implementation of the measures, including the results of an audit conducted at the entity's expense by an independent and qualified auditor selected by the entity. Note that sanctions arise in the event of infringements of the national provisions adopted pursuant to this Directive, and these sanctions must be effective, proportional, and dissuasive. Only a properly functioning critical infrastructure can ensure proper economic development, which is why the aforementioned Directives and their proper implementation in the national system of individual EU Member States are important legal tools.

2. The concept of safety

Inextricably linked to the concept of critical infrastructure is security, the absence or weakening of which can adversely affect the operation of critical infrastructure. Security is a fundamental element in the functioning of a state and the life of its citizens. The civilisational development and scientific and technological progress seen in recent decades implies that, in theory, citizens should feel much safer. However, the development of modern technologies, especially in the field of information technology and the so-called digital space, can at the very least cause citizens to be concerned about excessive interference in their private lives. Additionally, and especially in light of the considerable social unrest and armed conflicts in Europe and across the world, a paradigm shift in security thinking has been observed in recent years.

Regarding the etymology of the term "security", it is derived from the Latin term "*sine cura*" (*securitas*), and according to the dictionary definition, security is considered to be the so-called 'state of not being threatened'. According to the Dictionary of National Security Terms, security is 'a state of affairs that provides a sense of certainty and guarantees for its preservation and a chance for improvement'. One of the basic human needs is a situation characterised by the absence of risk and of the possibility of loss of important things that a person particularly values, such as

health, work, respect, feelings, and material goods.[26] Security is also defined as: 'the totality of conditions and institutions that protect the state and citizens from phenomena threatening the legal order', and as 'the protection of the system from attacks on the basic political institutions of the state'.[27] Maslow included the need for security in the second most important group of human needs, just after basic physiological needs. The following figure presents Maslow's pyramid of needs.

Figure 1. Maslow's pyramid

According to this author, 'If no need is satisfied, so that only physiological needs dominate in the organism, all other needs simply cease to exist or are relegated to the background'. Based on this argumentation, a question arises: is it the case that only after the basic needs have been satisfied, that is, physiological and safety needs, that other important needs appear?[28]

Still on the definition of the concept of security, it can be considered on three main levels, as follows: the ontological approach, related to the nature of security and where the basic element is the so-called existence and subjectivity; the epistemological approach, which attempts to identify the scientific cognition of the concept of "security" in its two dimensions (i.e. realistic and idealistic); the object-oriented approach, relating to the meaning of the term "security", which is framed in various sciences, including security sciences or defence sciences.[29] Security can also be con-

26 Pawłowski, Zdrodowski and Kuliczkowski, 2020, p. 20 et seq.
27 *Słownik Języka Polskiego PWN* [Dictionary of the Polish Language PWN], word: "security". [Online]. Available at: https://sjp.pwn.pl/słownik/bezpieczeństwo (Accessed: 27 July 2023).
28 Maslow, 2006, pp. 63–68.
29 Zdrodowski, 2019, pp. 48–50; See also: Brodie, 1949, p. 477; Zięba and Zając, 2010, p. 8.

sidered in relation to both its objective and subjective dimensions, the first being related to the objective state of the absence of physical danger.[30] Meanwhile, the subjective dimension relates to the state of consciousness of a certain subject/group, referring to a projection concerning the awareness of the perception of security. Security has also been described in terms of its internal security (i.e. the stability and harmony of a state) and external security (i.e. the absence of threats to the state and its citizens from external actors).[31]

2.1. Division of security

The concept of "security" is also interdisciplinary and transnational, and the Dictionary of Terms in the Field of National Security – developed by employees of the General Staff of the Polish Army, the Naval Academy, and the National Defence Academy based on literature presenting the views of doctrine representatives – systematises and presents a dozen of security concepts. Among the most important categories, there are the following:

- Global security, concerned with ensuring the security of all humanity and involving the major economic and military powers;
- Regional security, encompassing the security of countries in a particular region.
- National security, describing the survival of the state, including, inter alia, the freedom to pursue national interests.
- Military security, ensuring the ability to defend a given area and 'a state of awareness' in which the existing, projected, or possible level of military threat does not cause fear for the preservation of recognised values, the realisation of fundamental interests, and the achievement of strategic goals. This is based on the belief in the effectiveness of own and other actors' implemented and planned actions, and on the protective and defensive capabilities possessed.[32]
- Economic security, ensuring high efficiency in the development and functioning of the national economic system.
- Political security, consisting of activities related to the political dialogue conducted between countries and aimed at a country's security stability.
- Public security, referring to a status within the territory of a state made possible by efforts to provide organised protection and defence for persons and property against existing threats.
- Internal security, describing a state achieved by the actions of state bodies aimed at creating the most favourable international environment for a particular country, as well as strengthening its international position and image.

30 Kołodziejczyk, 2007, p. 228.
31 Zięba, 2001, pp. 217–219.
32 Sadowski, 2015, p. 125.

– External security, consisting of the achievement of a state as a result of the actions of state bodies, aims to create the most favourable international environment for the country in question as well as to strengthen the country's international position and image.[33]

The concepts of international and national security are also noteworthy, the former being defined as follows,

> a state characterised by the absence of objectively existing threats and subjective concerns, and by the concerted efforts and actions of the international community to protect certain state and non-state (social) values by means of norms, institutions and instruments that ensure the peaceful settlement of disputes and the creation of economic, social, environmental and other prerequisites for dynamic stability and the elimination of threats". In turn, national security, identified with state security, is defined as "one of the basic areas of state functioning (activity) intended to enable the survival, but above all the development and freedom to pursue national interests in a specific security environment (conditions), by meeting challenges, exploiting opportunities, reducing risks and countering all kinds of threats to its interests.[34]

Therefore, security is, on the one hand, a continuous process, and, on the other hand, a status (i.e. associated with the absence of danger) that requires authorised bodies to ensure its maintenance.[35]

An important aspect concerning national security is the need to preserve its sovereignty and independence. The recent events related to the long-lasting, extremely expansive, and unauthorised foreign policy of the Russian Federation – as exemplified by the armed conflict in Georgia in 2008, the conflict in Ukraine in 2014 that resulted in the illegal annexation of Crimea, and the recent hostilities in Ukraine, showcase the importance of a country's internal security and the need to protect critical infrastructure. Significant for international security are also the recent developments related to the hostilities conducted between Palestine and Israel. Certainly, 2023 has brought about the need for a change in the approach of EU Member States, including Poland, to the perception of security, as well as the need for a remodelling based on the current situation beyond the EU's eastern borders and, in particular, the actions taken by the Russian Federation and Belarus. An important aspect in the area of security is the anti-terrorist measures taken by EU Member States, which in turn relate the intensification of threats of this kind.

At this point, mention should be made of the period of Poland's political transformation from to 1989/1990, when it was one of the first European countries to release itself from the influence of the Soviet Union, which started to effectively disintegrate

33 Kaczmarek, Łepkowski and Zdrodowski, 2009, p. 14.
34 Kaczmarek, Łepkowski and Zdrodowski, 2009, p. 25.
35 Kukułka, 1995, p. 198 et seq.

on 16 November 1988, with the declaration of the sovereignty of Estonia. This disintegration process would see its ending only on 26 December 1991, when the Soviet Union passed a declaration of its self-dissolution. In Poland, its socio-political transition in the 1990s had a significant impact on its security issues, including those of an international nature. Authors dealing with these issues have pointed to the following as the main factors associated with the increase in crime and the decrease in security in the country: historical factors regarding the long-standing development of crime;[36] social factors, among which the dominant role was played by the collapse of values and authorities; a high level of acquiescence in the commission of certain types of crime, particularly of a fiscal and financial nature;[37] the public's demand for illegal services and goods that were previously unattainable for the average citizen.[38] Other factors were economic in nature and included structural and ownership changes, growing unemployment in a free market economy, increased crime in large cities (including criminal and tax crimes), and social stratification associated with the impoverishment of part of the population.

Meanwhile, the legal issues in Poland contributed to the inability to eliminate members of criminal groups, and some examples of these issues include the following: the failure to adapt its legal regulations to the prevailing market situation; the excessive liberalisation of laws, including those of a tax, criminal, economic, and procedural nature; the insufficient powers of law enforcement agencies to prevent crime and ensure an effective fight against it; the lack of effective methods to counter the intimidation of witnesses,. Other factors that associated with security issues in Poland were organisational/institutional factors, some of which were as follows: ineffective reform and reorganisation of law enforcement agencies,[39] which lacked sufficient competence and resources to combat members of organised crime group; cooperation of government officials (e.g. police, customs, tax authorities, and the UOP) with members of organised crime groups;[40] insufficient equipment and training of law enforcement officers, especially the for those in the police department;[41] lack of cooperation and coordination between services involved in combating crime.[42]

The international factors that influenced security issues in Poland resulted from, among other things, the points in the following list: the opening of the country's borders;[43] the socio-economic development in Europe;[44] the influx and penetration

36 Ocieczek, 2023, pp. 75–101; Mądrzejowski, 2005, pp. 53–54.
37 Sklepkowski and Woźniak, 1997, pp. 115–135.
38 Kossowska, 2002, p. 588; Laskowska, 2011, p. 379; Hołyst, 2000, p. 312.
39 An example of completely unjustified actions taken on the part of the management of the Ministry of the Interior and the KGP was the dissolution on April 6, 1990, of the Bureaus for Combating Economic Crime at the level of the KGP and the Provincial Headquarters of the Civic Militia. See: Rau, 2002, p. 53.
40 Pływaczewski, 1992, pp. 39–40; Bagieński and Gontarczyk, 2013, p. 18 et seq.
41 Pieprzny, 2007, p. 117.
42 Laskowska, 2011, pp. 164–165.
43 Hołyst, 2000, pp. 813–820.
44 Pływaczewski, pp. 3–9.

of organised crime groups from Europe, especially from the former countries of the so-called Eastern Bloc;[45] population migration;[46] the collapse of the Soviet Union; the entry of Poland into the structures of the EU;[47] the lack of multilateral and bilateral international agreements;[48] deliberate actions on the part of Russian authorities, which made use of their special services (i.e. the Federal Security Service, also known as FSB, and Main Directorate of the General Staff of the Armed Forces of the Russian, also known as GRU) to attempt to destabilise the economic, political, and economic situation in Poland.

As can easily be seen, some of the factors described here still exist in some European countries today, which can cause mutual destabilisation, as least to some extent, on the international stage. At the beginning of the 1990s, the majority of the Polish population expressed concerns about their sense of security. Still, this situation seems to have improved significantly since 2000, when Poland became a full member of the North Atlantic Treaty Organization (NATO) and aspired for its membership in the EU. Meanwhile, the results of an Eurostat survey conducted with EU Member States shows that the problem of safety in large cities still exists in the United Kingdom (30.8%). Disturbingly, high results were also recorded for Bulgaria (25%), Germany (13%), Belgium (16%), the Netherlands (15%), Greece (12%), and France (15%). Thus, it seems that Poland's western neighbours, like the Belgians and the British, are facing lower levels of sense of security within large cities. Similarly, the Swedish government is considering amending legislation to protect citizens from organised crime. Furthermore, according to the 2023 Crime Index, the most dangerous cities in Europe were Bradford in the United Kingdom, Marseille in France, and Catania in Italy.[49]

2.2. Terrorism

This section concludes by discussing the issue of terrorism, which has evolved over recent decades along with technological progress and the adaptation to the prevailing geopolitical context. Although this subject will be explored in another separate study, it is worth mentioning certain aspects related to this phenomenon. The Polish legislation, in Art. 115 § 20 of the Penal Code, defines terrorist offences as being punishable by imprisonment of at least five years, and offences committed with the purpose of the serious intimidation of many people, forcing a public authority of the Republic of Poland or of another state or an authority of an international organisation to take or to refrain from taking certain actions, causing serious

45 Gurov, 1990, p. 779 et seq; Gawenda, 2013, pp. 79–86; Rapacki, 2005; Świerczyński, 1997, pp. 187–198.

46 Gałek, 2001, p. 71; Sklepkowski, 1997, pp. 155–175.

47 Pływaczewski et al., 2011.

48 Laskowska, 2006, p. 334.

49 Europe: crime Index by City 2023. [Online]. Available at: https://www.numbeo.com/crime/region_rankings.jsp?title=2023&region=150 (Accessed: 4 October 2023).

disturbance to the system or economy of the Republic of Poland, another state or an international organisation, as well as the threat of such an act. Importantly, owing to the increasing terrorist threats, the Act of 10 June 2016 on Anti-Terrorist Activities[50] came into force on 2 July 2016, and according to the adopted assumptions,

> the basic aim of the regulation was to increase the effectiveness of the Polish anti-terrorist system, and thus increase the security of all citizens of the Republic of Poland, inter alia, through: strengthening the mechanisms for the coordination of activities, clarifying the tasks and areas of responsibility of individual services and bodies and the principles of cooperation between them, ensuring the possibility of effective action in the event of suspicion of an offence of a terrorist nature, including in the area of preparatory proceedings, ensuring response mechanisms adequate to the type of threats occurring and adapting criminal provisions to new types of terrorist activities.[51]

The Act introduced, among other things, a universally applicable and NATO-adapted four-level system of alert degrees for terrorist threats and cyberattacks. In addition, new types of terrorist offences were introduced, including, inter alia, the following: participation, for the purpose of committing a terrorist offence, in a training course that may enable the commission of such an offence (Art. 255a § 2 of the Penal Code); disseminating or publicly displaying content that may facilitate the commission of a terrorist offence, or for the purpose of gaining access to such content with the intent that such an offence be committed (Art. 255a § 1 of the Penal Code); setting up or leading an organised group or association with the aim of committing a terrorist offence (Art. 258 § 4 of the Penal Code). In the field of counterterrorism, important international legal acts normalising these issues include those outlined herein:

1. European Convention on the Suppression of Terrorism, drawn up on 27 January 1977, in Strasbourg;[52]
2. International Convention for the Suppression of the Financing of Terrorism of 9 December 1999;[53]
3. International Convention Against the Taking of Hostages;[54]
4. Convention on the Physical Protection of Nuclear Material;[55]
5. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism;[56]

50 *Act of 10 June 2016 on anti-terrorist activities*, 2016.

51 *Ustawa o działaniach antyterrorystycznych* (omówienie) [The Act on Anti-Terrorism Measures (Overview)], no date.

52 It entered into force on 4 August 1978, while Poland ratified the Convention on 30 January 1996 with effect from 1 May 1996.

53 *International Convention for the Suppression of the Financing of Terrorism of 9 December 1999*, 1999.

54 *International Convention Against the Taking of Hostages*, 1979.

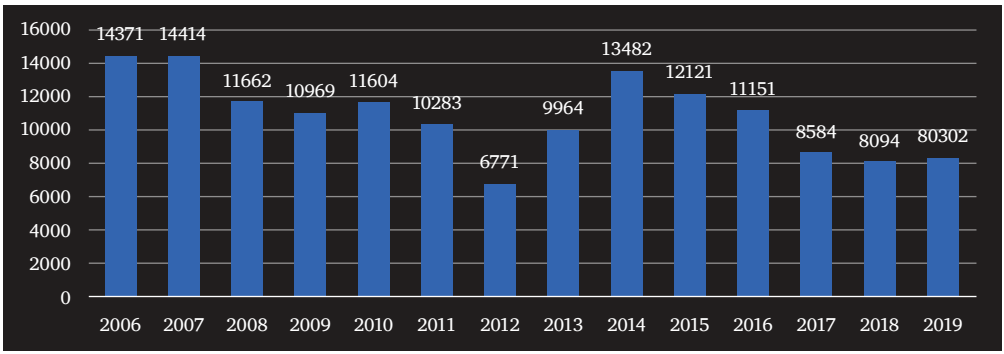
55 *Convention on the Physical Protection of Nuclear Material*, 1979.

56 *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198)*, 2005.

6. Council of Europe Convention on the Prevention of Terrorism of 16 May 2005;[57]
7. International Convention for the Suppression of Terrorist Bombings;[58]
8. Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism of 22 October 2015;[59]
9. Council Decision (EU) 2018/889 of 4 June 2018, on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism;[60]
10. Council Decision (EU) 2018/890 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism.[61]

As is widely believed, 2001 became a watershed year for global terrorism in terms of, among other things, globalisation and reach, as that year saw one of the largest terrorist attacks in the history of the United States of America.[62] The chart below illustrates the number of terrorist attacks worldwide during 2006–2019.

Chart 1. Number of terrorist attacks worldwide during 2006–2019[63]



As can be seen, the reduction in terrorist attacks dates from 2011–2013, perhaps related to the elimination of the most notorious terrorist, Osama bin Laden, which took place on 2 May 2011. However, from 2014, when there was the annexation

57 *Council of Europe Convention on the Prevention of Terrorism of 16 May 2005.*
58 *International Convention for the Suppression of Terrorist Bombings*, 1997.
59 *Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism*, 2015.
60 *Council Decision (EU) 2018/889 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism.*
61 *Council Decision (EU) 2018/890 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism.*
62 Karolczak, 2022, p. 10.
63 Author's numbers based on data in the following link: https://www.statista.com/statistics/202864/number-of-terrorist-attacks-world-wide/ (Accessed: 10 October 2023).

of Crimea by the Russian Federation authorities, and up until 2016, the number of terrorist attacks has definitely increased. It should be noted that the most active terrorist groups that carried out attacks worldwide in the years 2019 and 2020 were the Islamic State of Iraq and the Levant, the Taliban, Al-Shabaab, the Communist Party of India-Maoist, and Boko Haram.[64]

Similar to Poland, Hungary has also introduced changes to its anti-terrorism legislation. On 7 June 2016 the Hungarian parliament amended the constitution and revised several laws in response to terrorist threats. A terrorist emergency provision was also added to the Basic Law, which was introduced by the government and approved within 15 days by the parliament, with a two-thirds majority. This provision allows for the use of the national military for counterterrorism activities, and for the government to impose a curfew, restrictions on vehicle traffic, a ban on mass events, reinforce border protection, and secure tighter control of the Internet and postal communication. An Anti-Terrorism Information and Crime Analysis Centre (also known as TIBEK) was also established to collect and analyse data on public security threats.[65]

3. European Union Security Strategy (2020–2025)

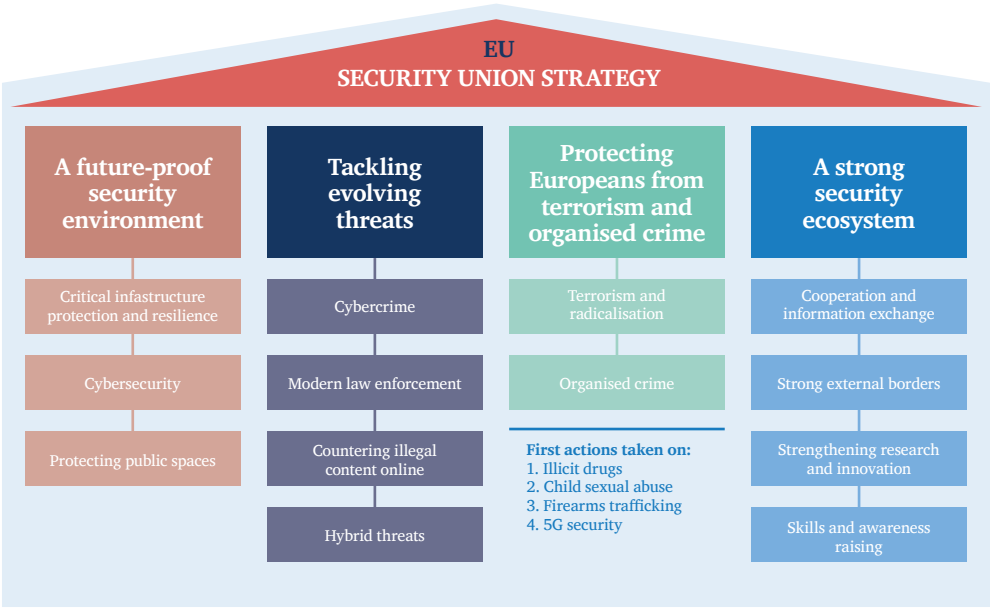
The European Security Union plays an important role in the security of the EU. This entity aims to ensure that EU security policy reflects changes in security threats in Europe, build long-term and sustainable resilience, and secure the involvement of EU institutions, agencies, governments, the private sector, and individuals in a whole-of-society approach. On 24 July 2020, the EU Security Strategy for 2020–2025 was published, the key pillars of which are the following:

- Focus on the fight against terrorism and organised crime, including organised crime, terrorism, and radicalisation.
- Provide a security environment that will stand the test of time and, in particular, tackle issues relating to critical infrastructure, cybersecurity, and public space protection.
- Build a strong safety ecosystem, including by improving research and innovation.
- Act in the face of changing threats such as hybrid threats, illegal content on the Internet, cybercrime, and modern law enforcement.[66]

The following diagram shows the most important elements of the Strategy.

64 Dyvik, 2022.
65 Sadecki, 2016.
66 Balcewicz, 2020.

Chart 2. European Union Security Strategy Source[67]



On 13 December 2022 an interim report on the implementation of the EU Security Strategy was adopted. It emphasised that most of the strategy's tasks had been discussed, albeit achieving its full impact on security would require action to implement the agreed upon legal solutions in individual national legislations, including the NIS 2 Directive (i.e. strengthens security requirements, including on incident response and crisis management) and the CER Directive (i.e. covers the physical critical resilience of entities to man-made and natural hazards).[68] Within the framework of the aforementioned report, the sabotage of the Nord Stream gas pipeline and the resulting risks have received special attention. Importantly, and as further elaborated in the Critical Infrastructure Report, the NIS 2 Directive covers a wide range of sectors, including energy, transport, banking, finance, market infrastructure, banking, and health.

Important elements in the framework of the EU Security Strategy are the resilience of critical infrastructure and the creation of a legal framework capable of strengthening, both physically and digitally, such infrastructure. Therefore, public–private stakeholder cooperation for the proper maintenance of security seems crucial.

67 Available at: https://cyberpolicy.nask.pl/strategia-bezpieczenstwa-ue-2020-2025/ (Accessed: 12 October 2023).

68 *Communication from the Commission to the European Parliament and on the Fifth Progress Report on the implementation of the EU Security Union Strategy*, 2022.

4. National Security Strategies (1990–2020)

Another aspect, this time of a national nature, related to security – and which encompasses, inter alia, the protection of critical infrastructure – is the national security strategies prepared since 1990 in Poland, initially called the Defence Doctrine of the Republic of Poland. These documents play an exceptionally important role in the context of security issues within the EU and the NATO. These strategies are part of the framework of international security in Poland, considering a broad definition of the term. Still, the basis of this strategic planning has changed in Poland through the Act of 11 March 2022 on the defence of the homeland (that is, Thz. U. from 2024. 248). Currently, an olive-strategic Defence Directive of the Republic of Poland and other implementing documents are envisaged for the National Security Strategy.

This Strategy begins its history with the aforementioned socio-political changes. In 1990, for the first time, a document called the Defence Doctrine of the Republic of Poland was prepared. It was then adopted by a resolution of the Committee for the Defence of the Country on 21 February 1990, based on Art. 5(2)(1) and Art. 6 of the Act of 21 November 1967, on the Universal Obligation to Defend the People's Republic of Poland.[69] The Doctrine sets out directions for Poland's defence and security policies, and its basic premises set out that the purpose of creating this document was to 'guarantee the most vital interests of the Polish Nation: security, the right to live in peace, the independence and sovereignty of the state, and the integrity and inviolability of its territory'. In this document, particular attention was paid to geopolitical issues, particularly Poland's strategic location, as well as the need to build a Polish defence doctrine together with Western allies in order to secure the nation's territorial integrity. According to the second part of the document, Poland, in accordance with the Charter of the United Nations, undertook to renounce the use of force and the threat of its use in international relations, not to initiate hostilities against another state or an alliance of states, and not to participate in war on the condition that it or its allies do not become the object of an armed attack. Important aspects recognised in the Defence Doctrine were the need to develop mutual international guarantees and security obligations, the introduction of early warning systems, and the need to secure the efficient and rapid coordination of forces and measures with respect to existing threats, both during peacetime and in the event of war.

> The doctrine was the result of a kind of homework of a very belated lesson on state defence within an alliance (…) Firstly, the Warsaw Pact in 1990 was no longer an alliance, but a group of states calling themselves members of the Warsaw Pact, with practically no knowledge of any rules of joint action, and at the same time not

69 *Act of 21 November 1967 on Universal Obligation to Defend the People's Republic of Poland, Journal of Laws.*

knowing what to do in the new conditions. Secondly, a belated lesson, because there was no longer any chance to implement the solutions adopted.[70]

At the same time, the Defence Doctrine can be considered to having been developed during a transitional period, during which Poland launched a search for new solutions and a new approach, while at the same time trying to distance itself from the Warsaw Pact. According to General Koziej's controversial assessment, the operational tasks of the armed forces were not formulated very fortunately and were limited to defensive operations only; this was supposedly, in his words, related to the aftermath of the introduction of the Warsaw Pact War doctrine in 1987, which favoured a defensive character of operations. In the General's opinion, such an approach could have had negative consequences for the efficiency and effectiveness of the Polish armed forces.[71] This Doctrine that emerged during a period of socio-political transformation was a peculiar novelty for Poland, and was in line with its "relaxation" tendencies on the one hand, while it showed clear tendencies towards the construction of pan-European alliances in terms of ensuring national security on the other hand. The Defence Doctrine also covered the security system and described that it was responsible for several key areas of the country's functioning, including the protection of the military, political, social, administrative, and economic fields, as well as civil defence and state protection. However, this document did not consider issues concerning the protection of critical infrastructure.

Other documents directly related to security policy in Poland were those on the assumptions of the Polish security policy and the security policy and defence strategy of the Republic of Poland. The Polish National Defence Committee adopted these documents on 2 November 1992. Work on the Defence Doctrine was undertaken by an inter-ministerial team appointed by the President of the Republic of Poland on 5 August 1991 and organised at the Polish National Security Office. The assumptions of the Polish security policy were divided into six main segments, as follows: basic assumptions, integration with Western Europe, international security regime, new regional cooperation, and internal security. The basic assumptions described that:

the Republic of Poland treats its borders as inviolable and has no territorial claims on its neighbours. It respects the sovereignty of other states and renounces the use of force, including the threat of force, in bilateral relations with other states. Poland wishes to cooperate particularly closely with its neighbouring states.

A fundamental aspect of these assumptions regarding the integration of Poland with Western Europe was the question of Poland's future membership in the European Communities, which was important from the point of view of sovereignty and economic development. Regarding regional cooperation, attention was drawn to the need for Poland to develop cooperation with Hungary, the Czech Republic, and Slovakia. In connection with the social and economic changes occurring in Poland,

70 Koziej and Brzozowski, 2015, p. 19.
71 Koziej, 2008b.

particular attention was also paid to internal security, specifically regarding the transition to a free market economy, the rapidly growing crime rates, emigration, and environmental degradation. Security policymakers also did not lose sight of the range of threats that could arise from the so-called process of change in the East, or the radical regime transition. In terms of security aspects, attention was paid to the process of demilitarisation (disarmament), the creation of multinational armed forces, and the elimination of an atmosphere of military insecurity. According to the adopted strategy, the main factor for stability and security was being part of NATO, while the long-term factor and priority was to secure Poland's membership in the European Community.

Regarding the main assumptions about Poland's defence strategy, the document indicates the need to prepare, develop, and maintain the state's defence infrastructure, secure public defence preparedness, and make Polish armed forces ready to engage in defence and intervention activities in case of need. The concept of defence, in terms of the so-called non-military defence links, primarily concerned the protection of citizens against catastrophic industrial risks, natural disasters, and the effects of warfare. An important role of defence was also indicated to the National Civil Defence, as an extra-military defence link, as it was entrusted with the coordination of activities of all forces and means serving to protect the life and property of the population and cultural assets – within the framework of the state defence system. The powers of civil defence are also listed in detail, with some particularly noteworthy ones being described herein: planning undertakings for the protection of the life and health of the population; protecting workplaces, public utilities, and cultural assets from the effects of warfare; organising risk detection in this area; warning and alerting the population and its evacuation; preparing protective facilities; organising rescue and decontamination operations. The management of the state's defence was entrusted to the President of the Republic of Poland, the Prime Minister, and the Council of Ministers.

The above-mentioned basic tenets of the 1992 Security Strategy were different from those in the previous 1990 Defence Doctrine, at least with regard to possible threats. In this respect, there were no references to global conflicts in favour of local or regional conflict, and there was also a lot of space devoted to the socio–political transition, the disintegration of the Eastern Bloc, and the resulting possible tensions or destabilisation.

Finally, after many years of efforts by Poland – as the efforts started on 10 April 1992, during the first meeting of the NATO Military Committee, a recurring meeting that would eventually be attended by the Ministers of Defence and the Chiefs of Staff of Central and Eastern European countries on February 1999 – the President signed, with the prime minister's prior countersignature, the Act of Accession of the Republic of Poland to the North Atlantic Treaty.[72] During the political and economic transition period of Eastern Europe, especially after the collapse of the Soviet

72 Dereń, 2016, pp. 17–30.

Union and the Warsaw Pact, the United States of America, with its great military and technological potential, played an important role in security policy. The United States of America regarded Europe as a strategic partner, while acknowledging that there was minimal security against armed conflict in Eastern European states. The result of this approach was the question as to whether the United States of America would assist countries such as Hungary, Poland, and the Czech Republic with their admission to NATO. Nonetheless, on 16 February 1995, the National Security Revitalization Act was passed in the House of Representatives of the U.S. Congress, which expanded NATO to include Poland, Hungary, the Czech Republic, and Slovakia. In Section 603 of US policy, item 1 indicated that the United States should continue its commitment to play an active leadership role in NATO. Point 2 of the resolution stated that, in terms of policy, it should join with the NATO allies in redefining the role of the alliance in the post-Cold War world, considering the following:

> (A) The fundamentally changed security environment in Central and Eastern Europe.
> (B) Need to reassure all states about the alliance's defensive nature and the desire of its members to cooperate with former adversaries.
> (C) Emerging security threats from the proliferation of nuclear, chemical, and biological weapons of mass destruction and their means of delivery.
> (D) Continued challenges to the interests of all NATO member states from unstable and undemocratic regimes with hostile intentions.
> E) Dependence of the global economy on stable energy supplies and free trade.

Regarding the participation of new partners, including Poland and Hungary, in accordance with Point 5 of the resolution:

> – that Poland, Hungary, the Czech Republic, and Slovakia should be in a position to further the principles of the North Atlantic Treaty and to contribute to the security of the North Atlantic area in the near future, and, in accordance with Article 10 of such Treaty, should be invited to become full NATO members, provided these countries---.
> (A) meet appropriate standards, including (…).[73]

The relevant document on Poland's security strategies following its accession to NATO was the Defence Strategy by the Council of Ministers, adopted on 23 May 2000. In terms of basic security policy objectives, the strategy included the following key topics: guarantee the independence, sovereignty, territorial integrity of the state and the inviolability of its borders; guarantee the protection of the democratic constitutional order, including, in particular, the fullness of rights and freedoms and the security of citizens of the Republic of Poland; create the best possible conditions for the comprehensive and stable social and economic development of the country, the well-being of its citizens, the preservation of the national heritage, and the development

73 *H.R. 7 (104th): National Security Revitalization Act.*

of national identity; and contribute to the building of a lasting, just peace order in Europe and worldwide, based on the values of democracy, human rights, the rule of law, and solidarity. Regarding the conduct of security policy principles, the following came to the fore in this document: a comprehensive approach to national security issues; implementation of security policy with respect for the Polish Constitution and international law; a security policy guided, inter alia, by the values, ideals, and principles enshrined in the North Atlantic Treaty and the European Treaties in their actions on the international scene; the close link between national security and the security of NATO countries and EU Member States.[74] Similar to the previous security strategy, this strategy also emphasises the significant role of NATO and the issue of integration with the EU. In the sphere of defence operations, the above strategy distinguished between preventive and stabilisation actions, crisis response, and warfare, which should carried out in the event of possible aggression.

The 2003 National Security Strategy was adopted on 22 July 2003 and was signed by the President of the Republic of Poland on 8 September 2003. The need to develop and implement this new Strategy was connected with the outbreak of war in Iraq and the consequent participation of the Polish military, and with the issue of joining the structures of the EU in the near future.[75] The Strategy document begins with a chapter entitled "New Challenges", which presents the objectives of the state's policy and are unchangeable and concerned with maintaining the inviolability of borders and territorial integrity. This chapter emphasises Poland's participation in NATO and the guarantees associated with entry in EU structures. In the area of national threats, issues related to the so-called atypical threats, whose sources, often non-state actors, are difficult to identify, were signalled. The development processes in the field of ICT were also identified, as well as how they may entail certain threats, such as to the stability of the financial, capital, and economic situation of Poland. The general assumptions, which are described in the second chapter of the aforementioned document, point to the fact that the boundaries between the external and internal aspects of security were blurring at the time. Simultaneously, Poland committed to contributing to international security. The third chapter, titled "Tasks of state services", presents the need to continuously strengthen international relations with the United States of America, NATO, and the European Union. In the field of internal security, the issues of improving public safety through legislative changes, increasing the number of officers, changing the organisational structures of police, and ensuring the cooperation between the police and local authorities were signalled. Important issues such as the protection of ICT infrastructure and computer crime (novum) were not omitted. The fourth chapter, concerning the economic foundations of state security, discusses issues related to finance, budget, economy, infrastructure, environment, and education. With regard to critical infrastructure, it was assumed the following:

74 *National Security Strategy of the Republic of Poland 2000*, p. 1.1.1 et seq.
75 Lasoń, 2007, p. 57.

> efforts to maintain the proper condition of Polish infrastructure are one of the conditions for ensuring adequate defence potential and national security, both internal and external. In the coming years, it is necessary to increase the state's efforts to modernise the transport infrastructure, including the construction of motorways and expressways, sustainable development of railway transport, construction of airports and airstrips and the navigation system, changes in the structure and volume of transshipment of sea and inland shipping and land-sea transport and logistics chains. It will be necessary to intensify efforts to provide infrastructure on the eastern border of Poland, which will become the external border of the EU area.[76]

Both strategies do not sufficiently distinguish strategic and national interests. For obvious reasons, such as the war in Iraq, terrorist attacks in New York on 9 September 2001, and Poland's application to join EU structures, the issues of Poland's international activity were comprehensively described.[77] In addition, the tasks of the Polish armed forces were presented in a disorderly manner, and no holistic approach to the state security system was presented.[78]

In April 2007, another National Security Strategy of the Republic of Poland was adopted by the Council of Ministers. In the introduction, it reads as follows:

> '(…) the Republic of Poland is a safe country (…)'. It should be emphasised that since 1 May 2004 Poland has become a full member of the European Union structures, which certainly influenced the shape of the developed strategy. Moreover, it was emphasised that the National Security Strategy of the Republic of Poland, correlated with allied strategies, i.e. the NATO Strategic Concept and the European Security Strategy – constitutes the basis for the development of executive strategic directives, in particular the Political-Strategic Directive of the Republic of Poland, strategies of individual domains of national security, strategic plans of defence reaction and crisis management as well as long-term programmes of transformation of the state security system, including programmes of non-military defence preparations and programmes of development of the armed forces.[79]

The Strategy is divided into four main parts, which are devoted to such aspects as those outlined herein: national interests and strategic objectives of the Republic of Poland in the field of security; determinants of the national security of the Republic of Poland; the concept of national security; sectoral goals and objectives; the National Security System of the Republic of Poland. Regarding Poland's strategic objectives, the strategy referred to the common security interests of the countries centred around NATO and the EU. According to point 16, the main strategic objectives

76 Koziej, 2008a.
77 Trofimowicz-Kalinowska, no date, p. 145.
78 Koziej and Brzozowski, 2015, pp. 32–34.
79 *National Security Strategy of the Republic of Poland 2007*, Para. 5 of the Introduction.

included the following: ensuring the independence and territorial inviolability of the Republic of Poland and its sovereignty in deciding the internal affairs of the nation's life, its organisation, and the state system; creating conditions for civilisational and economic development; determining the capacity of the nation and the state to act; ensuring a sense of legal security for the citizens of the Republic of Poland.[80] Much attention has been paid to Poland's energy security in the context of the increasing threat of political exploitation of energy resources. The starting point in this respect, which dates to problems occurring in as early as 2007, was the need to ensure the diversification of supply and the use of alternative energy sources (Chapters 2.1, 2.2, and 3.6 of the Strategy). Other identified and indicated threat directions were terrorism, international crime (including organised crime), and threats of an environmental nature.

In the field of internal security, the strategy pays attention to the question of the ability to respond adequately to threats. The issue of critical infrastructure, both in terms of both development and protection, has not escaped attention. In this area, priority has been given to the need to develop a transport and communication infrastructure (Section 3.6, pt. 73) to ensure ecological security (Chapter 3.7) and IT and telecommunication security (Chapter 3.8). It should be acknowledged that this Strategy dealt with the system of national security in an exceptionally broad and detailed manner, paying attention to economic threats (e.g. in the field of raw material supplies and energy security).

On 5 November 2014, at the request of the Prime Minister, the President of the Republic of Poland approved the 2014 National Security Strategy of the Republic of Poland, which replaced the 2007 version. The 2014 National Security Strategy consisted of four main chapters, which were focused on the following: Poland as a security actor; security environment; strategic action concept and operational strategy; a strategic preparation concept with a preparation strategy. As rightly contested by Trofimowicz-Kalinowska '(…) the authors of the document (National Security Strategy of the Republic of Poland of 2014 r.) noted more challenges than threats, which indicates a positive assessment of Poland's security environment'.[81] Unfortunately, subsequent years have negatively verified the approach of the authors of this strategy in this regard, considering, for example, the extremely aggressive foreign policy of the Russian Federation, the armed conflict in Ukraine triggered by it (2014 sic!), and the migration crisis at the Polish–Belarusian border. An important aspect concerning this 2014 Security Strategy, as was the case in the 2007 Strategy, was the emphasis on Poland's membership in the Euro-Atlantic and European structures, which in turn determined the directions of both the threats and key fields of Poland's development. Regarding military cooperation, the United States of America once again occupied an important place, as did the desire to seek ties with countries such as Lithuania, Latvia, Estonia, Romania, and the Nordic Group. It was also

80 *National Security Strategy of the Republic of Poland 2007*, Chapter 1.2 Point 16.
81 Trofimowicz-Kalinowska, no date, p. 145 et seq.

emphasised that, in terms of security and relations with the Russian Federation, the so-called freedom to choose own development path, including its political and military alliances, should be guaranteed. The national interests outlined in the 2014 Strategy included the following:

> – To have an effective national security capability to ensure preparedness and capacity to prevent, including deter, defend, and protect against, as well as recover from, threats.
> – Individual and collective protection of citizens against threats to their life and health and against damage, loss, or degradation of their essential assets (tangible and intangible).
> – To ensure the free exercise of citizens' freedom and rights without detriment to the safety of others and the security of the state and to ensure national identity and cultural heritage.
> – To ensure the sustainable and balanced development of the country's social and economic potential, with particular attention to the protection of the natural environment and the living and health conditions of the population as the basis for living.

It is worth emphasising the factor indicated in the 2014 Strategy that is directly related to the protection of critical infrastructure, namely: 'ensuring the lasting and sustainable development of social potential and economic state, with particular emphasis on environmental protection natural environment and the living and health conditions of the population as the basis existence', which is described in Chapter I, Point 1.2. Examples of strategic objectives in the field of ensuring security, which are largely related to the protection of critical infrastructure, have been focused on, among other topics, the following in this document: maintaining and demonstrating the readiness of the integrated national security system to seize opportunities, address challenges, reduce risks and counter threats; improving and developing the national crisis management system to ensure its internal consistency and integrity, and to enable seamless cooperation within the crisis management systems of international organisations to which Poland is a member; protecting Poland's borders, which are the external border of the EU; protecting public order. Other important aspects were improving systemic solutions for preventing and combating terrorism and the proliferation of weapons of mass destruction; ensuring the safe functioning of the Republic of Poland in cyberspace and ensuring energy and climate security and the protection of the environment, biodiversity, and natural resources, especially water resources; shaping the country's spatial development in a way that increases resistance to a variety of threats, especially military, natural, and technological threats.[82]

Another element included in the security strategy was the protection of critical infrastructure. According to section 4.3(132) on the so-called protection subsystem,

82 *National Security Strategy of the Republic of Poland 2014*, Chapter 1.2, Point 12.

> (…) The protection of the state's critical infrastructure requires structuring the legislation to create a single category of critical infrastructure facilities. This entails the need for changes in provisions for facilities subject to mandatory protection and those subject to special protection. Consistent legislation ensures that the resilience of all critical infrastructure elements is enhanced, which is the responsibility of a statutorily established critical infrastructure protection authority. New legislation should also create a system of real incentives for owners of critical infrastructure to invest in security.

This chapter defines the purpose of protection subsystems, which refer to the organisational, technical, and training development efforts related to the protection of the population, public order, and proper crisis management. In this respect, the role and key tasks of various institutions is outlined, as shown herein: justice; special services; bodies involved in countering and combating terrorism and extremism; authorities competent for cyber security; law enforcement services as well as critical infrastructure protection services; public safety services related to rescue and civil protection; border services; authority protection services and public administration.

In terms of strategic activities, chapter three of the Strategy presents priority directions for Poland, as follows: ensuring readiness and demonstrating determination to act in the sphere of security and defence; supporting processes to strengthen NATO's collective defence capabilities; developing the EU's Common Security and Defence Policy; strengthening strategic partnerships; supporting selective participation in the activities of the international community.[83] In summary, the 2014 National Security Strategy of the Republic of Poland, was a continuation and, in a way, a development of previous national strategies. However, some people criticised the way threats were presented, which, in their opinion, were too scattered throughout the strategy. In addition, as aforementioned, this strategy included more challenges than threats.[84]

At the request of the President of the Council of Ministers on 12 May 2020, the President of the Republic of Poland introduced a new National Security Strategy of the Republic of Poland, which replaced the 2014 Strategy. The main assumptions of this 2020 Strategy defined a comprehensive vision for shaping the national security of Poland in all dimensions. In addition, it considers the so-called subjective aspect, understood as the combination of the internal and international dimensions of security, as well as the physical aspect, considering all the dimensions of the functioning of the national security system. This strategy is in line with both the values described in the Constitution and the so-called context of Poland's presence in NATO and the EU.[85] The latest Security Strategy is divided into four key pillars, which are those described herein:

83 *National Security Strategy of the Republic of Poland 2014*, Chapter III.
84 Trofimowicz-Kalinowska, no date, p. 153.
85 *National Security Strategy of the Republic of Poland 2020*, Warszawa, 2020. p. 9.

– Pillar I: Security of the state and citizens
– Pillar II: Poland's international security system
– Pillar III: National identity and heritage
– Pillar IV: Social and economic development, and environmental protection.

The description of the essential pillars of the strategy is preceded by an introduction, which discusses topics such as the security environment of values, national interests, and strategic objectives in the context of national security. With regard to the description of the security environment, the first problems addressed are the Russian Federation's pursuit of a neo-imperialist policy, which led to the illegal annexation of Crimea, aggression against Georgia, and unauthorised actions in eastern Ukraine. In addition, it is mentioned that the Russian Federation conducts activities below the threshold of war (of a hybrid nature) that carry the risk of creating conflicts (e.g. unintentional, resulting from a sudden escalation as a result of an incident, especially a military one), as well as comprehensive and complex actions by non-military means (e.g. cyberattacks and disinformation activities) with the aim of destabilising the structures of Western states and societies and cause divisions among allied states. Unfortunately, the last sentences of the strategy have been fully confirmed by the recent events that took place in Ukraine and the Moldovan region. In addition, the dangers arising from the development of new technologies, including digital technologies, and their creation of a dangerous space for the manipulation of information and disinformation, have been noted. Regarding Poland's critical infrastructure, such as power plants and transmission networks (especially electricity, gas, and gas storage networks), the Strategy noted that the development of oil and fuel transmission and storage networks to date was insufficient. The introductory part of the strategy also highlights issues concerning the need for Poland to be firmly embedded in transatlantic and European structures, and to develop bilateral and regional cooperation with key partners. The 2020 Strategy also addresses topics pertaining to financial security, economic stability, health protection, and safety threats in the area of environmental protection (Pillar IV, pp. 33–35).

In the 2020 Strategy, the national interests are defined by four key points, as follows: (1) guarding the independence, territorial integrity, sovereignty, and security of the state and its citizens; (2) shaping an international order based on solidarity, cooperation, and respect for international law, and providing guarantees for Poland's secure development; (3) strengthening the national identity and guarding the national heritage; (4) securing the conditions for sustainable and balanced social and economic development and environmental protection.[86]

The most elaborate of the Pillars of the 2020 Strategy is Pillar I, in which there are descriptions about national security management; state resilience and common defence; cybersecurity; information space. Particular attention should be paid to the second chapter of Pillar I, focused on increasing the state's resilience to threats

86 *National Security Strategy of the Republic of Poland 2020*, Warszawa, 2020, p. 11.

through the creation of a system of universal defence, based on the efforts of the whole nation, and building an understanding of the development of the resilience and defence capabilities of the Republic of Poland. Section 2.8 draws attention to the need to implement a model for the protection of critical infrastructure, which in turn should be based on ensuring the continuity of its operation and services. Pillar II recommends, in the field of critical infrastructure, that the transport network should be developed to ensure an even saturation of infrastructure (especially in areas with limited transport accessibility to the TEN-T core) and a comprehensive network. These recommendations relate to the construction of the Polish section of the Via Carpatia, improvements in access to border crossings on the eastern border of the EU (Pillar II, Chapter II, Point 2.8), the expansion of seaports (Point 2.11), and the construction of the Central Communication Port and its inclusion in the national transport system (Point 2.13). With regard to the development of the aforementioned new technologies and the resulting threats, the 2020 Security Strategy recommends building the state's resilience to threats, including those of a hybrid nature, as well as enhancing its ability to protect the cybersphere. The suggestions for actions in this direction include conducting scientific research, continuously raising public awareness in this area, and obtaining the capability to conduct a full spectrum of military operations in the cyberspace. Pillar II of the 2020 National Security Strategy broadly coincides with the topics in the previous 2014 Strategy.

Pillar III should be regarded as the novel part of the Strategy, as its themes of identity and national heritage were addressed in a new way. This Pillar greatly focuses on strengthening the national identity, which is rooted in Christian heritage and universal values.

Pillar IV addresses the following topics: health and family protection; migration policy; economic security; energy security; environmental protection; scientific and technological potential. Regarding the protection of critical infrastructure, a particularly important issue presented in Pillar IV relates to energy security; this has become an important issue in light of recent events, particularly the aggressive war waged by the Russian Federation supported by Belarus against Ukraine, as it led to various economic sanctions being imposed by EU Member States on the Russian Federation. In accordance with Point 4, the key tasks of Poland are those outlined here: expand and modernise its energy generation capacity and electricity transmission and distribution networks to ensure continuity of supply (Point 4.1); increase the diversification of sources of crude oil and natural gas supplies (Point 4.2); increase the capacity, work safety, and range related to oil and fuel pipelines, as well as the capacity of fuel and oil depots (Point 4.3); continue the diplomatic, legal, and administrative activities aimed at stopping the construction of transmission infrastructure that increases the dependence of the Central European region on gas supplies from the Russian Federation (Point 4.4).

A very important provision of the 2020 Strategy from the perspective of state security is related to migration policy, which has become a significant problem in most EU Member States in recent years. Pillar IV, Point 2, describes the need:

> to develop and pursue a comprehensive migration policy, coordinated with the security, economic and social policy, taking into account both the current and projected needs of the labour market, integration of migrants into the Polish society, ensuring maintenance of social cohesion, as well as counteracting possible threats to public order and security related to migration processes.[87]

As far as national security strategies are concerned, one must agree that they should consider the assessment horizon – which should cover a period of five or six years and be shorter than one generation – and the assessment system – which should provide a general and specific view, and consider security-relevant opportunities, challenges, risks, and threats.

5. Conclusion

The security and protection of critical infrastructure in Poland are important issues and must be ensured, and this requires engaging in activities associated with ensuring physical, technical, personnel, ICT, and legal security. Specifically, it is key to draft and implement business continuity and restoration plans, referring here to sets of organisational and technical measures leading to the maintenance and (if necessary) restoration of functions performed by critical infrastructure.[88] Another important element in the protection of critical infrastructure is ensuring appropriate cooperation among Poland's institutions at the strategic, operational, and management levels, and at the international level. In terms of national regulations, important ones include those involved in ensuring a high common level of cybersecurity within the EU (NIS2; 14 December 2022), and the Critical Entity Resilience Directive (CER) (14 December 2022), which repealed Council Directive 2008/114/EC. The early detection of problems, resilience building efforts, and increasing citizens' awareness of the importance of securing the protection of critical infrastructure are also crucial steps toward securing the security of said infrastructure. Additionally, efforts should be made to develop research and thus use innovative solutions in this area.

As highlighted in the EU Security Strategy 2020–2025, it has become necessary, among other things, to do the following: adapt EU security systems to new threats; establish a joint cyber unit; improve law enforcement in the area of computer forensics as well as to counter hybrid threats. An extremely important aspect in the context of

87 *National Security Strategy of the Republic of Poland 2020*, Warszawa, 2020, p. 32.

88 *Resolution No. 210/2015 of the Council of Ministers of 2 November 2015, on the adoption of the National Programme for the Protection of Critical Infrastructure, with Annex No. 1 on standards to ensure the efficient functioning of critical infrastructure – good practices and recommendations*.

ensuring the security of critical infrastructure is also related to upholding its functionality, which may prove crucial in the face of the above man-made and natural threats. It should be emphasised that there is no "golden" means to guarantee the complete protection of critical infrastructure. Instead, such security is achieved by combining various elements, including the diversity of legal solutions in the field of critical infrastructure protection, engaging a significant number of entities responsible towards its protection and tackling an exceptionally large number of threats (i.e. natural and man-made). Therefore, only the introduction of 'good practices' in the field of critical infrastructure protection can bring the expected results in the form of minimising threats and ensuring the continuity of services and supplies of goods. An example of a 'good practice' is certainly the unification of law at the EU level and making efforts to promote international cooperation; for instance, joint training and exercises with other nations may contribute to ensuring appropriate immunity to critical infrastructure, improving related incident prevention, resilience, and timely recovery. Finally, it is worth mentioning that an extremely important aspect in the protection of critical infrastructure is ensuring legal security, which involves implementing appropriate security procedures, checking them, and systematically adapting them to real threats.

References

Bagieński, W., Gontarczyk, P. (2013) *Żelazo w dokumentach MSW i PZPR* [„Żelazo" scandal in the documents of the Ministry of Internal Affairs and the Polish United Workers' Party]. Warszawa: IPN.

Brodie, B. (1949) 'Strategy as a science', *World Politics*, 1(4), pp. 467–488; https://doi.org/10.2307/2008833.

Bryła, M. (2000) 'Porozumienie, zorganizowana grupa, związek przestępczy jako formy organizacyjne przestępczości zorganizowanej' [Agreement, organised group, criminal association as organisational forms of organised crime], *Prokuratura i Prawo*, 2000/3, pp. 24–39.

Dereń, J. (2016) 'Warszawski szczyt NATO projekcją sojuszniczego bezpieczeństwa' [The Warsaw NATO summit is a projection of allied security], *Rocznik Bezpieczeństwa Międzynarodowego*, 10(1), pp. 17–32.

Domański, Z. (2017) 'Bezpieczeństwo socjalne' [Social security], *Journal of Modern Science*, 2(33), pp. 367–384.

Ficoń, K. (2007) *Inżynieria zarzadzania kryzysowego. Podejście systemowe* [Engineering Crisis Management. A case-based approach]. Warszawa: Bell Studio Sp. z o. o., p. 76.

Gałek, D. (2001) 'Migracje legalne i nielegalne na wschodniej granicy RP' [Legal and illegal migrations on the eastern border of the Republic of Poland] in Białocerkiewicz, J. (ed.) *Wschodnia granica RP zewnętrzna granica Unii Europejskiej* [Eastern border of Poland External border of the European Union]. Kętrzyn: Materiały konferencyjne, p. 71.

Gawenda, A. (2013) 'Rosyjska przestępczość zorganizowana faktycznym zagrożeniem dla Polski' [Russian organised crime an actual threat to Poland], *Studia Prawnicze i Administracyjne*, 1(5), pp. 79–86.

Glen, A. (2011) 'Zagrożenia bezpieczeństwa narodowego RP' [Threats to the national security of the Republic of Poland] in Piątek, Z. (ed.) *Edukacja na rzecz bezpieczeństwa, Wybrane problemy* [Security education, Selected issues]. Warszawa: CSIEE.

Gurov, A. (1990) *Profiesyolalnaya priestupnost. Proshloye i sovriemiennost* [Professional crime. Past and present]. Moscow: Psihologičeskaja biblioteka.

Hołyst, B. (2000) *Kryminologia* [Criminology]. Warszawa: Wydawnictwo Prawnicze PWN, pp. 813–820.

Jakubczak, R. (ed.) (2008) *Obrona narodowa w tworzeniu bezpieczeństwa Polski w XXI wieku: podręcznik do przysposobieniu obronnego dla studentek i studentów* [National Defence in the Creation of Poland's Security the 21st Century: a textbook on defence preparation for students]. Warszawa: Dom Wydawniczy Bellon.

Kaczmarek, J., Łepkowski, W., Zdrodowski, B. (eds.) (2009) *Słownik terminow z zakresu bezpieczeństwa Narodowego* [Dictionary of national security terms]. Warszawa: Akademia Obrony Narodowej.

Karolczak, K. (2022) 'Terroryzm XXI wieku – wybrane aspekty' [Terrorism in the 21st century – selected aspects], *Terroryzm – studia, analizy, prewencja*, 1(1), pp. 9–28; https://doi.org/10.4467/27204383TER.22.001.15417.

Kitler, W. (2010) 'Bezpieczeństwo narodowe. Podstawowe kategorie, dylematy pojęciowe i próba systematyzacji' [National Security. Basic categories, conceptual dilemmas and an attempt at systematization], in Piekarski, M., Zdziech, M. (eds.) Warszawa: Zeszyty problemowe TWO, 1(61), p. 52.

Kołodziejczyk, A. (2007) 'Bezpieczeństwo jako fenomen społeczny: pojęcie bezpieczeństwa, jego interpretacje i odmiany' [Security as a social phenomenon: the concept of security, its interpretations and variations], *Seaculum Christianum: pismo historyczno-społeczne*, 14/1, pp. 223–252.

Kosewska, A. (1978) 'Przestępczość w wielkim mieście' [Crime in the big city] in Batwia, S., Jasiński, J. (eds.) *Zagadnienia nieprzystosowania społecznego i przestępczości w Polsce* [Issues of social maladjustment and crime in Poland]. Wrocław: Zakład Narodowy im. Ossolińskich.

Kossowska, A. (2002) 'Zapobieganie przestępczości w Polsce w latach 90 – perspektywa kryminologiczna' [Crime prevention in Poland in the 1990s – a criminological perspective] in Czapska, J., Kury, H. (eds.) *Mit represyjności albo o znaczeniu prewencji kryminalnej* [The myth of repressiveness or the importance of crime prevention]. Kraków: Wyższa Szkoła Bezpieczeństwa, pp. 585–603.

Koziej, S., Brzozowski, A. (2015) *Strategie Bezpieczeństwa Narodowego RP 1990-2014. Refleksja na ćwierćwiecze.* [The National Security Strategy of the Republic of Poland 1990-2014. Reflections for a quarter of a century]. Warszawa: Wojskowe Centrum Edukacji Obywatelkiej im. płk. dyplm. Mariana Porwita.

Kukułka, J. (1995) 'Nowe uwarunkowania i wymiary bezpieczeństwa międzynarodowego Polski' [New conditions and dimensions of Poland's international security], *Wieś i Państwo*, 1995/1, pp. 198–199.

Laskowska, K. (2006) *Rosyjskojęzyczna przestępczość zorganizowana. Studium kryminologiczne* [Russian-speaking Organized Crime. A criminological study]. Białystok: Temida 2.

Laskowska, K. (2011) *Etiologia przestępczości zorganizowanej w Polsce* [Etiology of organised crime in Poland]. Warszawa: C.H. Beck.

Lasoń, M. (2017) Polska strategia bezpieczeństwa narodowego na początku XXI wieku [Polish national security strategy at the beginning of the 21st century], *Krakowskie Studia Międzynarodowe*, 2007/4, pp. 49–63.

Maslow, A. (2006) *Motywacja i osobowość* [Motivation and Personality]. Warszawa: PWN.

Mądrzejowski, W. (2015) *Przestępczość zorganizowana. System zwalczania.* [The Scheme of Counteracting]. Warszawa: Editions Spotkania Spółka.

Mierzejewski, J. (2011) *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych* [European security under the impact of globalisation]. Toruń: Wydawnictwo Adam Marszałek.

Ocieczek, G. (2023) *Instytucja świadka koronnego w ujęciu materialnoprawnym, karnoprocesowym i empirycznym* [The institution of a crown witness in material legal, criminal procedural and empirical terms]. Warszawa: Wyawnictwo Instytutu Wymiaru Sprawiedliwości.

Pawłowski, J., Zdrodowski, B., Kuliczkowski, M. (2020) *Słownik terminów z zakresu bezpieczeństwa narodowego.* [Glossary of terms related to national security]. Toruń: Wydawnictwo Adam Marszałek.

Pieprzny, S. (2007) 'Zmiany prawno-organizacyjne w Policji w latach 1990-2007' [Legal and organisational changes in the Polish Police in 1990-2007] in Szymaniak, A., Ciepiela, W. (eds.) *Policja w Polsce. Stan obecny i perspektywy. Tom I.* [Police in Poland. Present state and perspectives. Vol. 1.]. Poznań: Wydawnictwo Naukowe Wydziału Nauk Politycznych i Dziennikarstwa UAM.

Pływaczewski, E. (1992) *Przestępczość Zorganizowana i jej zwalczanie w Europie Zachodniej (ze szczególnym uwzględnieniem republiki Federalnej Niemiec)* [Organised Crime and its Fight in Western Europe (with Particular Reference to the Federal Republic of Germany)]. Warszawa: Wydawnictwo Prawnicze.

Pływaczewski, E. (2011) *Przestępczość Zorganizowana* [Organized Crime]. Warszawa: C.H. Beck.

Radvanovsky, R., McDougall, A. (2010) *Critical Infrastructure. Homeland Security and Emergency Preparedness*. London, New York: CRC Press.

Rapacki, A. (2005) 'Przestępczość zorganizowana w Polsce – subiektywne spojrzenie policjanta' [Organised crime in Poland – a subjective view of a policeman], *Policja: kwartalnik kadry kierowniczej policji*, 2005/1.

Rau, Z. (2002) *Przestępczość zorganizowana w Polsce i jej zwalczanie* [Organised crime in Poland and its fight against it]. Kraków: Wolters Kluwer.

Sadowski, S. (2015) *Bezpieczeństwo militarne Rzeczpospolitej Polskiej* [The military security of the Republic of Poland]. Warszawa: Repozytorium UKW.

Sklepkowski, L., Woźniak, D. (1997) *Zorganizowana przestępczość gospodarcza w Polsce* [Organised economic crime in Poland] in Pływaczewski, E., Świerczewski, J., (eds.) *Policja polska wobec przestępczości* zorganizowanej [The Polish police against organised crime]. Szczytno: Wydawnictwo Wyższej Szkoły Policji, pp. 115–135.

Skrabacz, A. (2012) *Bezpieczeństwo społeczne – podstawy teoretyczne i praktyczne* [Social security – theoretical and practical foundations]. Warszawa: Dom Wydawniczy Elipsa.

Świerczyński J. (1997) *Przestępstwa popełniane w Polsce przez obywateli państw powstałych po upadku Związku Radzieckiego* [Crimes committed in Poland by citizens of countries established after the collapse of the Soviet Union] in Pływaczewski, W., Świerczewski, J. (eds.) *Policja Polska wobec przestępczości zorganizowanej* [Police of Poland against organised crime]. Szczytno: Wydawnictwo Wyższej Szkoły Policji, pp. 187–198.

Szewczyk, T., Pyznar, M. (2010) 'Ochrona infrastruktury krytycznej a zagrożenia asymetryczne' [Critical infrastructure protection and asymmetric threats], *Przegląd Bezpieczeństwa Wewnętrznego*, 2(2), pp. 53–59.

Tyburska, A. (2011) 'Policja a ochrona infrastruktury krytycznej' [Police and the protection of critical infrastructure], *Zeszyty Naukowe WSOWL*, 3(161), pp. 143–162; https://doi.org/10.5604/01.3001.0002.3052.

Wadowski, J.S. (2018) 'Ochrona infrastruktury krytycznej. Geneza problemu' [Critical infrastructure protection. Genesis of the problem], *Organizacja i zarządzanie*, 2018/6, pp. 1237–1241.

Zdrodowski, B. (2019) 'Istota bezpieczeństwa państwa' [The essence of national security], *Annales Universitatis Pedagogicae Cracoviensis: Studia de Securitate*, 9(3), pp. 47–71.

Zięba R. (2001) *Instytucjonalizacja bezpieczeństwa europejskiego* [Institutionalisation of European security]. Warszawa: Wydawnictwo Naukowe Scholar.

Zięba, R., Zając, J. (2010) *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski* [Building an integrated system of national security for Poland]. Warszawa: Ministerstwo Rozwoju Regionalnego.

Zybertowicz, A. (2005) 'AntyRozwojowe Grupy Interesów: zarys analizy' [Anti-Development Interest Groups: outline of analysis] in Wesołowski, W., Włodarek, J. (eds.) *Kręgi integracji i rodzaje tożsamości [Integration circles and types of identity]*. Wydawnictwo Naukowe Scholar: Warszawa, pp. 1–22.

Legislation

Act of 21 November 1967 on Universal Obligation to Defend the People's Republic of Poland (1967) Journal of Laws, 1988, No. 30, item 207, as amended.

Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (2015) Official Journal of European Union, L 159/17, Ryga, 22 June 2015.

Annex No. 1, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008) Official Journal of the European Union, L 345/75, 23 December 2008.

Convention on the Physical Protection of Nuclear Material (1979) Vienna, 26 October 1979.

Council Decision (EU) 2018/889 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism (2018) Official Journal of the European Union, L 159, 22 June 2018.

Council Decision (EU) 2018/890 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (2018) Official Journal of the European Union, L 159, 22 June 2018.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008) Official Journal of the European Union, L 345/75, 23 December 2008.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198) (2005) Warsaw, 16 May 2005.

Council of Europe Convention on the Prevention of Terrorism (2005) Official Journal of the European Union, L 159/3, Warsaw, 16 May 2015.

Critical Entity Resilience (CER) Directive of 27 December 2022 (2022) Official Journal of the European Union, L 333/164, 27 December 2022.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022) Official Journal of the European Union, L 333/80, 27 December 2022.

Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022, amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (Text with EEA relevance), PE/42/2022/REV/1 (2022) Official Journal of the European Union, 27 December 2022.

H.R. 7 (104th): National Security Revitalization Act.

International Convention Against the Taking of Hostages (1979) New York, 17 December 1979.

International Convention for the Suppression of Terrorist Bombings (1997) New York, 15 December 1997.

International Convention for the Suppression of the Financing of Terrorism (1999) OJ. 263, items 2619 and 2620, New York, 9 December 1999.

National Security Strategy of the Republic of Poland 2000.

Protocol Additional to the Geneva Conventions of 12 August 1949.

Regulation (EU) 2022/2554 of the European Parliament and of the Counsil of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, (2022) OJ EU L 333/1, 27 December 2022.

Resolution No. 210/2015 of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure with Annex No. 1 on standards to ensure the efficient functioning of critical infrastructure – good practices and recommendations.

Weekly Copilation of Presidential Documents. US Government Printing Office. Washington DC.20402/ No. 3/ Vol. 29/ January, 25/ 1993.

Intermedia

Act of 10 June 2016 on anti-terrorist activities (2016) Journal of Laws 2016, item 904. [Online]. Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20160000904 (Accessed: 9 October 2023).

Balcewicz, J. (2020) 'Strategia Bezpieczeństwa UE 2020-2025' [EU Security Strategy for 2020–2025], *Cyber Policy*, 21 August 2020. [Online]. Available at: https://cyberpolicy.nask.pl/strategia-bezpieczenstwa-ue-2020-2025/ (Accessed: 12 October 2023).

Dyvik, E.H. (2022) 'Most active terrorist organizations worldwide in 2020, by number of attacks', *Statista*, July 2022. [Online]. Available at: https://www.statista.com/statistics/937553/terrorism-most-active-perpetrator-group-worldwide (Accessed: 10 October 2023).

Europe: crime Index by City 2023 (2023) *Numbeo*. [Online]. Available at: https://www.numbeo.com/crime/region_rankings.jsp?title=2023&region=150 (Accessed: 4 October 2023).

Green Paper on a European programme for critical infrastructure protection, Commission of the European Communities (2005) COM(2005) 576 final, Brussels, 17 November 2005. [Online]. Available at: http://eurex.europa.eu/LexUriServ/site/pl/com/ (Accessed: 21 August 2023).

Incydent na Morzu Czerwonym. Kluczowe kable przecięte [Incident on the Red Sea. Key cables cut] (2024) *Polsat News*, 5 March 2024. [Online]. Available at: https://www.polsatnews.pl/wiadomosc/2024-03-05/incydent-na-morzu-czerwonym-kluczowe-kable-przeciete/ (Accessed: 10 March 2024).

Jalonen, J. (2009) 'Dni, które wstrząsnęły Estonią' [The days that shook Estonia], *Eesti*, 12 May 2009. [Online]. Available at: www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html (Accessed: 21 August 2023).

Jędrak, J. (2022) 'Ile ofiar pochłonęła katastrofa w Fukushimie? Tysiące, ale z nieoczywistego powodu' [How many lives were claimed by the Fukushima disaster? Thousands, but for an unobvious reason], *smogLab*, 11 March 2022. [Online]. Available at: https://smoglab.pl/fukushima-ofiary-wplyw-na-srodowisko (Accessed: 24 August 2023).

Katastrofa w Czarnobylu [Chernobyl Disaster] (no date) *Centralne Biuro Antykorupcyjne*. [Online]. Available at: https://antykorupcja.gov.pl/ak/retrospekcje/retro/6351,Katastrofa-w-Czarnobylu.html (Accessed: 24 August 2023).

Koziej, S. (2008a) *Strategie Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 2003 i 2007 roku. Skrypt internetowy* [National Security Strategies of the Republic of Poland of 2003 and 2007], Warszawa: Skrytp Internetowy. [Online]. Available at: https://koziej.pl/publikacje/ (Accessed: 3 August 2023).

Koziej, S. (2008b) *Ewolucja bezpieczeństwa narodowego rzeczpospolitej Polskiej w latach dziewięćdziesiątych XX wieku. Skrypt internetowy* [Evolution of national security of the Republic of Poland in the 1990s.]. Warszawa: Skrypt Internetowy. [Online]. Available at: https://www.koziej.pl (Accessed: 3 August 2023).

Kuczabski, M. (2021) *Bezpieczeństwo psychiczne jednostki jako podstawa humanistycznego podejścia do bezpieczeństwa narodowego* [Psychological security of the individual as the basis of a humanistic approach to national security]. [Online]. Available at: https://www.researchgate.net/publication/354386492_Mental_security_of_an_individual_as_the_basis_of_a_humanistic_approach_to_national_security (Accessed: 2 August 2023).

National Security Strategy of the Republic of Poland 2003 (2003) Warsaw: Ministry of National Defence of Poland. [Online]. Available at: https://dataspace.princeton.edu/handle/88435/dsp016m311r75x (Accessed: 10 October 2023).

National Security Strategy of the Republic of Poland 2007 (2007) Warsaw: Ministry of National Defence of Poland. [Online]. Available at: https://dataspace.princeton.edu/handle/88435/dsp01g445cg59q (Accessed: 10 October 2023).

National Security Strategy of the Republic of Poland 2014 (2014) Warsaw: Biuro Bezpieczeństwa Narodowego. [Online]. Available at: https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf (Accessed: 10 October 2023).

National Security Strategy of the Republic of Poland 2020 (2020) Warsaw: Biuro Bezpieczeństwa Narodowego. [Online]. Available at: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf (Accessed: 10 October 2023).

Sadecki, A. (2016) 'Pakiet antyterrorystyczny na Węgrzech' [Anti-terrorist package in Hungary], *Ośrodek Studiów Wschodnich*, 15 June 2016. [Online]. Available at: https://www.osw.waw.pl/pl/publikacje/analizy/2016-06-15/pakiet-antyterrorystyczny-na-wegrzech (Accessed: 10 October 2023).

Słownik Języka Polskiego PWN [Dictionary of the Polish Language PWN]. [Online]. Available at: https://sjp.pwn.pl (Accessed: 21 August 2023).

Trofimowicz-Kalinowska, K. (no date) *Pojęcie bezpieczeństwa w strategii bezpieczeństwa narodowego Polski i Hiszpanii* [The concept of security in the National Security Strategy of Poland and Spain]. Core. [Online]. Available at: https://core.ac.uk/download/pdf/187227208.pdf (Accessed: 17 August 2023).

Wiech, J. (2021) 'Fukushima minuta po minucie. Co się stało w japońskiej elektrowni jądrowej' [Fukushima minute by minute. What happened at Japan's nuclear power plant], *Energetyka 24*, 11 March 2021. [Online]. Available at: https://energetyka24.com/atom/fukushima-minuta-po-minucie-co-sie-stalo-w-japonskiej-elektrowni-jadrowej (Accessed: 24 August 2023).

Reports and communication

Raport Rządowy RP skierowany do Sejmu RP (2000) 'Bezpieczeństwo i porządek publiczny' [Government Report to the Sejm of the Republic of Poland, Security and Public Order], Warszawa, 13 June 2000.

Heniff, B. (2004) 'CRS Report for Congress: Congressional Budget Action in 2004', *Congressional Research Service*, 27 December 2004.

Communication from the Commission to the European Parliament and the on the Fifth Progress Report on the implementation of the EU Security Union Strategy (2022) COM(2022) 745 final, Brussels, 13 December 2022.