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]

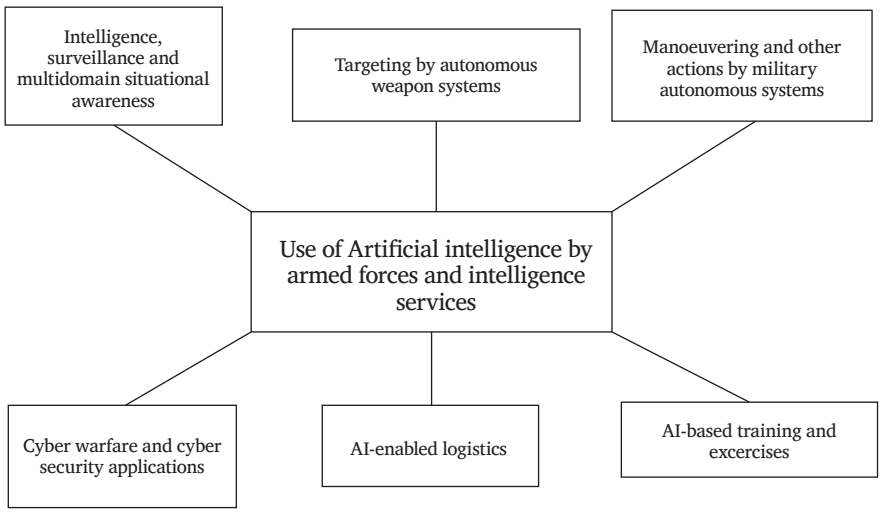
AI will contribute to military applications at tactical and strategic levels by analysing big data, optimising processes, and supporting planning. AI-enabled systems are capable of multitasking and can collect categorise, and transmit data, signals, images, and videos collected by drones.[24] This will 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.