Conference Proceedings

Conflicts in the Gray Zone
A Challenge to Adapt

MAY 9–10 2017, BUDAPEST, HUNGARY

Conference Proceedings

Conflicts in the Gray Zone
A Challenge to Adapt

MAY 9–10 2017, BUDAPEST, HUNGARY

Conflicts in the Gray Zone: A Challenge to Adapt
May 9–10 2017, Budapest, Hungary

Table of Contents

Rationale for the Conference

For nearly seven decades the political cohesion and military power of the Alliance has ensured the prosperity and security of the Euro-Atlantic region. However, the Alliance is currently being aggressively opposed both by emerging powers and by non-state entities in ways that are often far from peaceful, but fall short of any recognized threshold of conventional war. These confrontations pose a particular difficulty both for the NATO alliance and for some of its member states, since their political and military structures are optimized for prevailing in conventional conflicts. The biggest challenge is that the Alliance needs to operate and adapt at the same time.

The Scientific Research Centre of the Hungarian Defence Forces General Staff organized the conference to discuss this phenomenon, the spectrum of gray zone challenges, as well as the possible nation-state and alliance responses to them. Three main sub-topics suggested themselves:

- The security environment. In what direction is the security environment developing in the next 20 years? A widening gray zone with more ambiguity and uncertainty? A return of international war? A battlefield populated only by robots? A mixture of all of the above? Total chaos? How can the legal systems of the various nation-states adapt to the gray zone challenges? How can international law keep up with the changes?
- Societal and administrative responses to the challenge. How can a nation (or an alliance) respond to a gray zone challenge? What makes a state vulnerable to gray zone attack? How can the state reduce its vulnerability? How can it harden its civilian institutions and its administrative structures? How can it build societal resistance and resilience against such gray zone attacks as hybrid challenges, terrorism, or cyber-attacks?
- Military response to the challenge. How can the armed forces be prepared to meet gray zone challenges and prevail? How can a nation under grey zone attack take the fight to the enemy? How can a nation's armed forces be prepared to successfully handle either conventional war, or

grey zone, or internal security challenges? What are the defense policy, training and doctrinal implications?

The presentations, panel discussions and the final plenary session gave partial answers to some of these questions. This publication contains the papers the speakers prepared based on their presentations.

Disclaimer: the views and opinions summarized here are those of the participants; they do not reflect the views of their governments or parent organizations.

Conclusions and Recommendations

1.

Gray zone methods, tactics, and techniques are not new. The *emergence, integration, and enabling effects* of various new technologies have made them vastly more threatening today, than 50 or 100 years ago. The resulting threat is of a different order of magnitude than in the past.

Identifying the narrative or, rather, the narratives of a particular country is crucial to understanding. The more narratives there are in a country, the more unstable it is likely to be. For example, there are nine narratives in Pakistan, and nine in China. In Europe the number of narratives is increasing as a result of large scale migration. Instead of the various narratives converging, we see divergence, leading to instability – and lack of stability makes a country vulnerable to gray zone attacks.

Gray zone challenges often target the affected state's social cohesion, and exploit its vulnerabilities. The gray zone attack may be hard to define, because today's western society is generally uncomfortable with identifying and labeling a country or a non-state organization as the aggressor. Identifying the targeted society's vulnerabilities may be equally difficult, partly due to political blind spots and the reluctance to label fellow citizens as the enablers of foreign aggression. In any case, the identification of societal-based vulnerabilities that a foreign aggressor can exploit is a relatively new requirement.

Disaffected minority groups often do not identify with the state and reject the national identity. The aggressor may be able to exploit their disaffection. Encouraging members of the disaffected minority to participate in the affairs of the nation on an equal footing with the majority (e.g. serving in the armed forces) may reduce the social divide between the minority and the majority.

2.

In a well-conceived and well-executed gray zone operation the aggressor has the initiative. As long as the affected state remains in a reactive mode, it is at a grave disadvantage, because it is playing to the adversary's strengths, and

playing by his rules. Since the adversary's goal is to achieve his warlike objectives without the risks inherent in even the most carefully limited war, adopting effective deterrence measures will frustrate his calculus. If deterrence is not sufficient, raising the stakes by escalation to the level of conventional conflict may be the appropriate response in certain cases.

Most states, as well as most international organizations, have mechanisms to identify, and respond to, potential crises. However, these mechanisms are often ineffective: the information sharing regimes of the international organizations are often inadequate, and they do not cooperate well enough when responding to crises. For example, uncontrolled migration was identified 17 years ago as a potential problem, but it was left to the various national governments to deal with it. When the first waves of the migration crisis hit in 2015 Europe was surprised and unprepared.

National governments, as well as such international organizations as NATO must switch from reactive answers to pro-active behavior and should focus more to setting the agenda. In order to regain the initiative, they should play to their own strengths, as well as find the adversary's weakness. Their core values are a source of significant strength.

Timing is everything: whatever response a state decides to make, it must be made in a timely manner, because any delay benefits the aggressor. It may already be too late to make an effective response when the aggressor begins actual operations. This puts a premium on intelligence gathering by the states most likely to be exposed to gray zone challenges. The output of scientific research, in particular thorough analyses of gray zone lessons learned so far (e.g. the use of little green men in the Crimea), and new technologies, especially new electronic devices are key intelligence enables.

Since gray zone challenges appear to be the norm in the foreseeable future, all means and resources should be allocated to devising active defense responses and to regaining the strategic initiative. The challenges must be anticipated (fusing intelligence from a variety of key stakeholders is a key enabler), and must be incorporated into defense planning. As in most potential conflicts, the ideal solution is foresight and a proactive mindset (prevention). However, prevention is very difficult to achieve in the ambiguous environment.

States that have adopted a "total defense" concept, which addresses not only the defense of sovereign territory, but also the defense of all sectors that affect the stability of the society (economy, administration, judiciary, etc.),

and in which every citizen has a role to play, are the most likely to overcome a gray zone challenge.

3.

Legitimacy, credibility and *strategic communication* are three closely related key issues in a gray zone challenge. Although they apply to both the aggressor and the defender in equal measure, the conference considered them primarily from the defender's point of view.

The operational environment is characterized by ambiguity and uncertainty, as well as considerable legal uncertainty. This allows the aggressor to question the legitimacy of the defender's actions (or the legitimacy of the defender's very existence), and to attack his credibility.

Legitimacy and credibility are value judgments. They are subjective and competitive. They may be manipulated, and may change over time. They may be withheld from a state actor, even when its actions are entirely legal. Success may confer legitimacy in some cases. However, legitimacy acquired through success alone is ephemeral. Paradoxically, consistent defeat can also confer legitimacy and credibility, through the "martyr effect."

Clearly identifying the adversary, and reliably attributing such reprehensible acts to him as the use of human shields (incrimination) is an important step in obtaining legitimacy and credibility, and thus obtaining support from allies.

In the discussions of every panel, as well as in most presentations, the role of strategic communication received special emphasis. Good strategic communication plays a very significant role in gaining legitimacy and credibility. Conversely, legitimacy and credibility may be lost due to poor strategic communication, even if the state's actions are perfectly legal.

This puts the burden of responsibility on the government to establish and maintain professional and trustworthy news agencies and state-owned media to provide credible information to the public (both domestic and international), and to counterbalance fake media and any disturbing or misleading influence from other – adversarial – media outlets and agencies.

- To achieve these goals the government must seize control of the narrative, keep it under control before, during and after the conflict. Trying to discredit the adversary's narrative through counternarratives does not work very well. Suppressing his narrative by reshaping it, and offering alternative narratives are far more effective.

- When society gets used to fake news, it begins to question the truthfulness of all news. The government must make a special effort to minimize this outcome by offering both sides of the issues – this sets the parameters of what is valid news, while maintaining the authority to set those boundaries for public debate. This raises the question of how to ensure that fake news are filtered out. Setting up specialized units and organizations to identify and tackle fake news is a partial answer.
- Strong civil society and NGO sectors can articulate the voices and opinions of the local population, and they also play a role in shaping public opinion. Reaching out to them and obtaining their cooperation and assistance to influence public opinion is another partial solution.
- Creating synergies between civil society, the NGOs and government agencies may also help identifying the challenge in time, which in turn will contribute to shifting from reactive to a more pro-active stance.

4.

Reflecting the relative novelty of the concept of the gray zone, the conference was divided on the subject of definitions.

One school of thought holds that clear, sharp definitions are necessary to discuss gray zone conflicts and the appropriate strategy. Unless we adopt precise definitions, our response to the challenge will also be vague, fuzzy, and ineffective. For example, in military affairs the word "enemy" is reserved for a hostile foreign nation, its armed forces, and its citizens. In the gray zone / hybrid conflict context the use of this word is usually inappropriate. In a broader sense, the language we use for hybrid/gray zone challenges ought to be refined. To start with, hybrid conflict and gray zone conflict are two distinct phenomena: hybrid conflicts generally have a pronounced conventional element, which is usually absent in the gray zone.

The opposing school holds that the ambiguity of definitions is not a big problem: the lack of clearly articulated definitions is the essential character of new security environment. This ambiguity, and the discourse surrounding it, are symptoms of change. An effort to define some terms is a useful exercise, though. For example, does "gray zone" apply only to the proxy and targeted state, or does it also apply to the proxy's patron? A definition of the "enemy" (or an equally descriptive term for the adversary) is also important. Yet this view holds that there is no point in dwelling on definitions too long, or putting too much time and effort into them. Furthermore, adopting rigorous definitions may force us into a straitjacket, cramp our thinking, and limit our ability

to come up with new ideas to respond to gray zone challenges that do not fit the definitions.

Stepping beyond the subject of definitions, the relevance of the principles of war must be thoroughly investigated. Are the traditionally accepted principles appropriate in a hybrid / gray zone context? If not, what principles should be applied?

5.

As a pioneer and consummate gray zone actor, Russia came under close scrutiny by the conference.

Russia is frustrated by its technological and numerical disadvantage compared to the NATO, and by the extension of the alliance into the post-Soviet sphere. However, in gray zone operations it has found a way to advance its interests in a manner that best suits its capabilities.

- The objective is generally not to destroy, but to disrupt and render ungovernable the targeted country.
- Russian operations show an understanding of net-enabled warfare.
- Operations are multi domain, and whole spectrum, and they exploit the synergies obtainable through the integration of the economical use of force and the broad use of non-military tools. They are characterized by persistent deniability: the extensive use of proxies, and other covert means.
- The information domain is not limited to wartime – on the contrary, it is equal to other domains, it is a focal point in persistent operations and it is backed up by significant resources.
- Pressuring and influencing public opinion through effective information operations is considered the Center of Gravity in gray zone operations.
- Russia has anti-access and area denial (A2AD) capability, but no clear intention to use it.
- Conflict zones are interconnected: a conflict in the south is tightly connected to the Artic, etc.

Russian thinking about its new strategic toolbox is a constantly evolving and developing process. Operational experience (from Ukraine and Syria) is channeled into contemporary Russian military thinking, and is thus actively shaping it. However, real adaptation – a true mindset change – has not taken place in the Russian armed forces as a whole. Declared strategy might have changed, but the military culture (apart from very few elite units) is still very rigid.

Russia advances its interest by seeking out, probing, and exploiting the vulnerabilities of the western world. In order to regain the strategic initiative, the West must respond to the challenge. This also means that the "Gerasimov doctrine," which is of 2013 vintage, may already be outdated. In order to avoid the mistake of preparing for a past conflict, the systematic, thorough monitoring and analysis of Russian military thinking and capabilities are highly necessary.

6.

A cautionary note was struck by some participants. A mechanism for listening and dialogue is necessary both in peacetime and as crises unfold, in order to prevent an upcoming challenge to turn into a major conflict. Generally, we must listen more carefully to our counterparts – both our partners and our potential adversaries. We must recognize that our adversaries may also have valid and well-founded security concerns, and their gray zone challenge may be the result of our own failure to pay attention and acknowledge the validity of those concerns.

Identifying the adversary as the aggressor is not enough. In our own minds we may be the "good guys" and the adversary may be the "bad guy." However, this oversimplified, Manichean division is not sufficient for planning purposes. Furthermore, we must keep in mind that in the adversary's eyes, exactly the opposite applies: they are the "good guys" and we are the "bad guys."

Presentations

Peter Balogh

Gray Zone Activities – with a Focus on the Social Domain[1]

Abstract: This paper investigates some of the social aspects of the gray zone challenge through the patterns and mechanisms of hybrid threats that are either directly or indirectly linked to the societal dimension. It makes use of case studies to shed light on how ambiguity can emerge straight from social relations among actors, how divisive propaganda can operate in online media, resulting in a completely uncertain public discourse, and how the integrity of a civil sector can be disrupted. The primary objective is to carry out an empirical exploration, modelling or simulation which may lead to a more profound comprehension of the complex gray zone phenomenon, and contribute to the adaptability of societies being on the receiving end of a hybrid threat. Empirical investigation of gray zone operations in progress is neither an objective of this paper, nor is it possible, as these are dominantly covert activities, and due to the ambiguity surrounding them, the true nature of media events or a civil society movement is revealed only after the fact.

Introduction

Ambiguity seems to be one of the most characteristic features of gray zone or hybrid   conflicts (as they are referred to in the terminology of the United States and NATO, respectively).[2] Even the very origin of this rather complex

---

2   OSKARSSON, K. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." OPEN Publications 1/2. 2017 1–16. 6: footnote 4. – https://www.openpublications.org/single-post/2014/05/01/The-Effectiveness-of-DIMEFIL-Instruments-of-Power-in-the-Gray-Zone   and BRANDS, H. "Paradoxes of the Gray Zone". Foreign Policy Research Institute. 2016 – http://www.fpri.org/article/2016/02/paradoxes-gray-zone/, last accessed on 2017. 07. 07. 2., The Gray Zone. United States Special Operations Command White Paper. Public Intelligence. 2015   –

compilation of methods, tactics and strategic thinking is ambiguous. According to some argumentations the concept of the gray zone comes from Russia to distinguish a specific form of warfare applied by the United States against the country that resulted in a renewed approach to warfare in Russia to counter these challenges.[3] A similar concept – unrestricted warfare –which contains military and non-military methods of war comparable to the ones related to gray zone activities can also be found in Chinese military writings.[4] The unique way of war labelled by the expression of gray zone or hybrid proves to be an essential part of the approach followed by the USA – represented by the unconventional warfare methods applied by special operations forces.[5] Since the international order as it exists today is advantageous for the United States and the Western world, contemporary gray zone activities aim fundamentally to "*aggressively oppose this Western-constructed international order.*"[6] The most active state and non-state gray zone actors reflect this: Russia, China, Iran, North Korea; the Islamic State, Boko Haram.[7] So it is this international sphere where the gray zone activities conceptually emerge connected to the

https://publicintelligence.net/ussocom-gray-zones/, last accessed on 2017. 07. 07. 1., 4., "Report on Gray Zone Conflict". International Security Advisory Board. U.S. Department of the State. 2017 – https://www.state.gov/t/avc/isab/266650.htm – last accessed on 2017. 07. 07. 1.

3   "Report on Gray Zone Conflict" 3: footnote 5.
4   LIANG, Q., XIANGSUI, W. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999 – http://www.c4i.org/unrestricted.pdf
5   VOTEL, J. L., CLEVELAND, Ch. T., CONNETT, Ch. T., IRWIN, W. "Unconventional Warfare in the Gray Zone." *JFQ* 80/1, 2016. 101–109. – http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf – 102., 103., BRANDS. "Paradoxes of the Gray Zone." 3., The Gray Zone: 3., "Report on Gray Zone Conflict" 3: footnote 5., 13., FREIER, N. P. (ed.) Outplayed: Regaining Strategic Initiative in the Gray Zone, A Report Sponsored by the Army Capabilities Integration Center in Coordination with Joint Staff J-39/Strategic Multi-Layer Assessment Branch. Strategic Studies Institute, U. S. Army War College Press. 2016 – https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325 – 64–70., OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 16.
6   *The Gray Zone*. 5.
7   BRANDS. "Paradoxes of the Gray Zone." 2., OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 5–6., "Report on Gray Zone Conflict" 3, 16., VOTEL et al. "Unconventional Warfare in the Gray Zone." 102., FREIER, N. P. (ed.) *Outplayed.* 33–40., 41–55., *The Gray Zone*: 5.

global *objectives*, *interests*, *goals*[8] of the countries involved – may it be an intention to maintain or rather to modify the status quo.[9]

Gray zone or hybrid conflict encompasses a wide range of methods that can be applied in international competitive interactions.[10] Besides the traditional hard power,[11] further unconventional tactics and methods play a significant role – e.g. cyberattacks, information warfare, propaganda, political warfare, economic coercion, the use of proxy fighters, misinformation, deception – forming a challenge that is political and military at the same time.[12] The effectiveness of the hybrid tactics, however, comes from targeting the society itself.[13] The foremost objective of information operations and propaganda warfare,[14] for example, is to achieve a deep social impact[15] by sharing and spreading contradictory information in the media.[16] This can create uncertainty[17] about the actors, events and even facts which may result in the vulnerability of the society.[18] In this sense a gray zone conflict is more about the division in enemy opinion in a battle of the narratives.[19] So the society itself is the medium of hybrid information threats,[20] however in order to erode the political and social stability[21] the civil society can also be a target of gray zone attacks. Both transnational non-governmental[22] and local civil society

---

8   VOTEL et al. "Unconventional Warfare in the Gray Zone." 13, 102., OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 5–6., "Report on Gray Zone Conflict" 13., OBERNIER, J. A., SANDERS, F. A. "Enabling Unconventional Warfare to Address Grey Zone Conflicts". Small Wars Journal 9. 2016. – http://smallwarsjournal.com/jrnl/art/enabling-unconventional-warfare-to-address-grey-zone-conflicts – 1.

9   BRANDS. "Paradoxes of the Gray Zone." 2., 6., OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 6.

10   "Report on Gray Zone Conflict" 1.

11   HLATKY, S. v. "NATO's Public Diplomacy in the Grey Zone of Conflict". USC Center on Public Diplomacy. 2016. – https://uscpublicdiplomacy.org/blog/nato%E2%80%99s-public-diplomacy-grey-zone-conflict – last accessed on 2017. 07. 07. 2.

12   BRANDS. "Paradoxes of the Gray Zone." 2., 6., OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 6–7., "Report on Gray Zone Conflict" 2., VOTEL et al. "Unconventional Warfare in the Gray Zone"102., HLATKY. *"NATO's Public Diplomacy in the Grey Zone of Conflict."* 1.

13   *The Gray Zone:* 7.

14   OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 7.

15   HLATKY. *"NATO's Public Diplomacy in the Grey Zone of Conflict."* 1.

16   BRANDS. "Paradoxes of the Gray Zone." 4.

17   BRANDS. "Paradoxes of the Gray Zone." 2., *The Gray Zone:* 4.

18   OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 9.

19   "Report on Gray Zone Conflict" 2., OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 12.

20   OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 13.

21   OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 11.

22   "Report on Gray Zone Conflict" 4, footnote 6.

groups[23] are considered to be significant soft power actors in a the hybrid challenge.[24] It is an acknowledged tactic in unconventional warfare operations to give "*support to a resistance movement or insurgency against an occupying power or adversary government*"[25] and this way coercive means might come directly from the society itself – particularly if some elements of the civil sector can be manipulated by the aggressor.[26]

CASE STUDIES

The ambiguous network of the global war on terrorism

The subject of the first case study is the international coalition against terrorism. This global *collaboration* is a rather multifaceted one – at least if we consider the participants involved: the overall number of belligerents is 181: 132 countries from all regions of the world[27] fought or fight against 49 terrorist organizations, insurgent groups and even pirates[28] in several international

---

23   BRANDS. "Paradoxes of the Gray Zone." 5., OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 12.

24   OSKARSSON. "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." 12., HLATKY. *"NATO's Public Diplomacy in the Grey Zone of Conflict."* 2.

25   VOTEL et al. "Unconventional Warfare in the Gray Zone." 103.

26   VOTEL et al. "Unconventional Warfare in the Gray Zone." 108.

27   The US-led coalition against international terrorism includes the following states (in alphabetical order): Afghanistan, Albania, Algeria, Angola, Armenia, Australia, Austria, Azerbaijan, Bahrain, Belarus, Belgium, Benin, Bosnia and Herzegovina, Botswana, Bulgaria, Burkina Faso, Burundi, Cabo Verde, Cameroon, Canada, Central African Republic, Chad, China, Congo, Côte d'Ivoire, Croatia, Cyprus, Czech Republic, Denmark, Djibouti, Dominican Republic, El Salvador, Equatorial Guinea, Estonia, Ethiopia, Finland, France, Gabonese Republic, Georgia, Germany, Ghana, Greece, Guinea, Guinea-Bissau, Honduras, Hungary, Iceland, India, Indonesia, Iran, Ireland, Islamic Republic of The Gambia, Italy, Japan, Jordan, Kazakhstan, Kenya, Kingdom of Lesotho, Kingdom of Swaziland, Kosovo, Kuwait, Kyrgyzstan, Latvia, Lebanon, Liberia, Libya, Lithuania, Luxembourg, Macedonia, Madagascar, Malawi, Malaysia, Mali, Mauritania, Mauritius, Moldova, Mongolia, Montenegro, Morocco, Mozambique, Namibia, Netherlands, New Zealand, Nicaragua, Niger, Nigeria, Norway, Oman, Pakistan, Philippines, Poland, Portugal, Qatar, Republic of South Africa, Republic of South Sudan, Republic of the Sudan, Romania, Russia, Rwanda, São Tomé and Príncipe, Saudi Arabia, Senegal, Serbia, Seychelles, Sierra Leone, Singapore, Slovakia, Slovenia, Somalia, South Korea, Spain, State of Eritrea, Sweden, Switzerland, Taiwan, Tajikistan, Tanzania, Thailand, Togolese Republic, Tonga, Tunisia, Turkey, Turkmenistan, Uganda, Ukraine, Union of the Comoros, United Arab Emirates, United Kingdom, United States, Uzbekistan, Zambia, Zimbabwe.

28   The opponents of the coalition include the following organizations and groups (in alphabetical order): 1920 Revolution Brigades, Aal-Nusra Front, Abu Sayyaf, Ahrar al-Sham, Al-Itihaad al-Islamiya, Alliance for the Re-liberation of Somalia, Al-Mourabitoun, Al-Qaeda, Al-Qaeda in the Islamic Maghreb, Al-Qaida in Iraq (AQI), Al-Shabaab, Ansar al-Sharia (Libya), Ansar al-Sharia (Tunisia), Ansar al-Sunna, Ansar Dine, Asa'ib Ahl al-Haq, BIFF (Bangsamoro Islamic Freedom Fighters), Boko Haram, Harakat al-Shabaab Mujahedeen, Hizbul Islam, ISthe Islamic State (IS) ,

missions. Eleven international missions and operations are[29] analyzed, from 2001. 10. 07. (the starting date of the Afghanistan operations) to the still ongoing Operation Inherent Resolve.

I investigated the cooperation network of the states based on their participation in the missions and operations. It needs to be stated that the network I could draw from this research does not necessarily reflects the actual importance of the states in direct combat activities.[30] It could rather be interpreted as a nominal or *symbolic* partnership among nation states to overcome the global threat of terrorism.[31] The structure of the cooperation network proves to be rather complex, and notable differences can be observed among the participants (figure 1.). According to the quantitative indicators the United States of America plays the most important and central role in the cooperation, that is, the highest level of involvement can be measured in the case of the initiator. The mean value of degree centrality – strictly speaking the number of ties or links towards other countries in the cooperation network – is 96,4 coupled with a standard deviation of 54,8 (the lowest value is 8 links and the highest is 289 relations – in the case of the USA). Considering the distribution – in the light of the value range defined by the mean and the twofold ± standard deviation statistics – further countries can be identified as ones highly embedded in the network structure (e.g. Australia, United Kingdom, Spain).

IS – Libyan Provinces, IS - Wilayah Kavkaz, IS - Wilayah Khorasan, IS - Wilayat al-Jazair, IS - Wilayat Barqa, IS – Wilayah Gharb Ifriqiyyah, IS - Wilayat Sinai, Islamic Courts Union, Jabhatul Islamiya, Jaysh al_Mahdi, Jemaah Islamiyah, Jund al-Aqsa, Kata'ib Hizballah, Marka Group, Maute Group, MOJWA (Movement for Oneness and Jihad in West Africa), Moro Islamic Liberation Front, Mu'askar Anole, Naqshbandia, National Volunteer Coast Guard (NVCG), Puntland Group, Ras Kamboni Brigades, Salafia Jihadia, Somali Marines, Tahrir al-Sham, Taliban, Yemeni Pirates. Inter-Services Intelligence, the Pakistani intelligence organization occupies an ambiguous position: it actively supports some violent extremist organizations, and opposes others.

29   NATO—ISAF, Operation Enduring Freedom – Afghanistan (OEF-A), Operation Enduring Freedom – Philippines (OEF-P), Operation Enduring Freedom – Horn of Africa (OEF-HOA), Operation Enduring Freedom – Pankisi Gorge, Operation Enduring Freedom – Trans Sahara (OEF-TS), Operation Enduring Freedom – Kyrgyzstan, support for the Northern Alliance, Multi-National Force – Iraq, Combined Joint Task Force – Horn of Africa, Combined Joint Task Force – Operation Inherent Resolve.

30   It is particularly true if we consider that the objectives of some of the missions and operations included in the analysis were solely training (e.g. Operation Enduring Freedom – Pankisi Gorge), capacity building (e.g. Combined Joint Task Force – Horn of Africa) or access to physical infrastructure (e.g. airbase; Operation Enduring Freedom – Kyrgyzstan).

31   I am grateful for Spencer B. Meredith III for his comment using Afghanistan as a main example highlighting the possible difference between the involvement level of a certain country measured with degree centrality in the cooperation network and the actual significance of the same country in the process of achieving the goals of the war on terrorism.
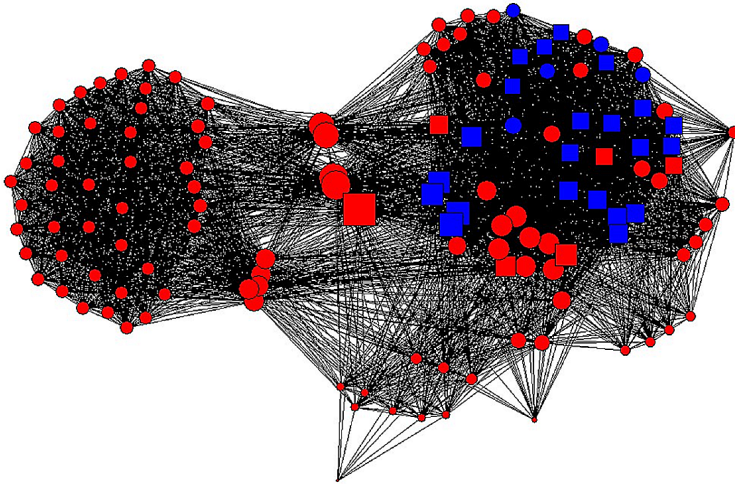
Figure 1.

Cooperation network of 132 countries in the global war on terrorism
Legend: blue = EU member state; square = NATO member state

Source: calculations by the author based on complex dataset

As for the structure of the differences among the countries participating in the global war on terrorism, macro-level organizational integration seems to be a clear factor as both in the case of European Union member states and the NATO member countries significantly higher level of involvement can be measured: compared to the mean value (96,4) the average degree centrality indicator of the EU member states is remarkably higher (147,1), and the NATO countries show an even greater level of participation with an average value of 162,3 relations (table 1.).

	degree centrality (number of relations)
not EU member states	83,4
EU member states	147,1
not NATO member states	78,7
NATO member states	162,3
mean	96,4

Table 1.

Higher involvement of EU and NATO states in the global war on terrorism

Source: calculations by the author based on complex dataset

It is also a clear empirical pattern that the status of the participating country in the globalized world order is roughly proportional to its position in the coalition against global terrorism. Investigating the Global Connectedness Index[32] a moderate positive correlation (R=0,53) can be observed indicating the tendency that the higher the rate of globalization, the higher the involvement in the global cooperation against terrorism is of the countries participating (figure 2).
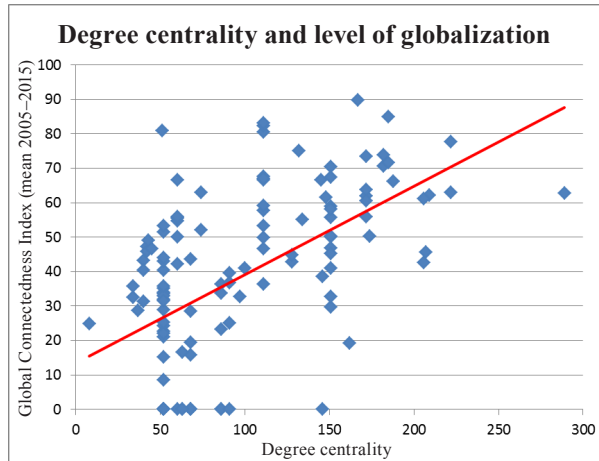
Figure 2.
Involvement in the war on terror and global connectedness

Source: calculations by the author based on complex dataset

A similar positive linear relation – although a much lower correlation coefficient (R = 0,22) – can be measured in the case of the global firepower of the countries (figure 3). The general pattern shows that the higher the level of military potential[33] of the country, the higher its degree centrality in the network

---

32   Mean values for the time period between 2005–2015 for that data is available. Source: own calculation based on the data of GHEMAWAT. P. ALTMAN, S.A. „DHL Global Connectedness Index 2016." Deutsche Post DHL, November 2016.
http://www.dhl.com/en/about_us/logistics_insights/studies_research/global_connectedness_index/global_connectedness_index.html#.VFff5MkpXuM

33   In order to make the general positive correlation recognizable between global fire power and the involvement level in the cooperation network against global terrorism I transformed the initial fire power index values which originally indicate higher military potential with lower – closer to zero – fire power index. I calculated the inverse values of global fire power (GFP) according to this function: $GFP_{inverse} = (GFP)^{-1}$.

proves to be. However the rather low correlation value expresses that there is a remarkably less intense connection which might be – at least partially – explained by the apparent outliers at the lower value range of the horizontal axis. That is, these countries are characterized by approximately the highest level of global fire power coupled with degree centrality values belonging to the lowest value range. Russia and China can be identified as the two outliers mentioned before which implies that two of the main gray zone actors of the world are integrated – at least in a certain level – into the US-led coalition against global terrorism. Specifically investigating this part of the graph around Russia and China a distinct sub-network can be explored. This partition of the whole network (figure 4.) incorporates 36 participating countries, including seven NATO member states – the USA and four European Union members amongst them –, and at the same time containing notable gray zone actors of Russia, China and Iran.
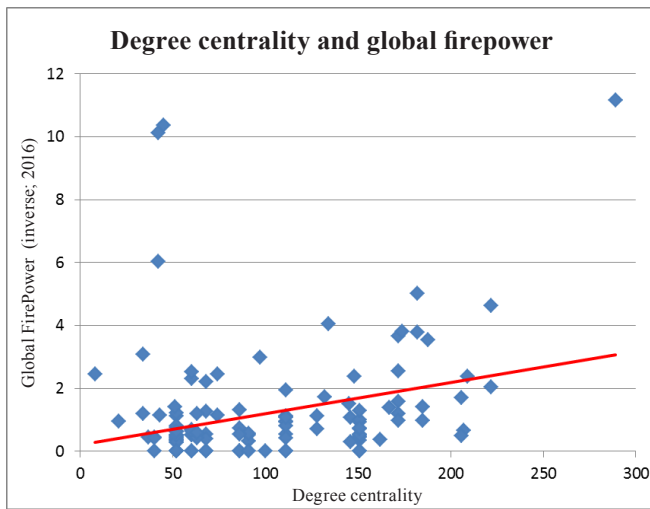
Figure 3.
Involvement in the war on terror and global firepower
Source: calculations by the author based on complex dataset

We can conclude from this analysis of the global war on terrorism that a higher level of involvement in the international cooperation network can be observed in the case of EU and NATO member states, the more globalized countries, furthermore the states possessing armies with more significant fire power. However a more interesting outcome of the analysis is that a distinc-

tive feature of gray zone activities can be empirically documented as the am-
biguous position of certain partners in the cooperation network is explored.
The fact that gray zone actors (Russia, China, Iran) are integrated into the
network implies a kind of '*friend and foe*' position (instead of '*friend or foe*'):
some of the countries committed to fight global terrorism are working *against*
their partners in other activities.
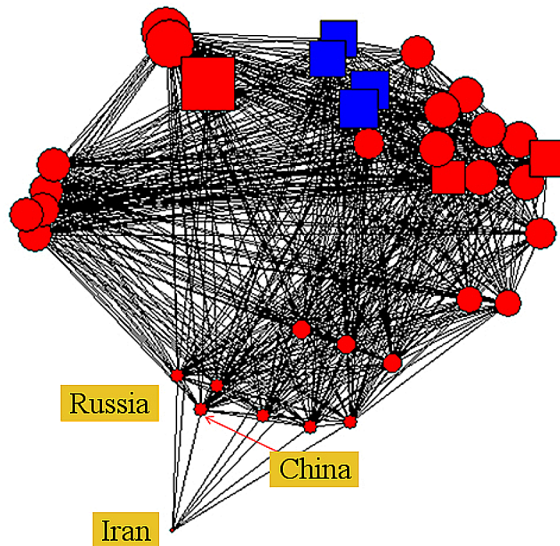
Figure 4.
*Sub-graph of the main gray zone actors in the U.S.-led coalition
against terrorism*

SOURCE: calculations by the author based on complex dataset

Uncertainty of online public discourse[34]

The next question I examine is some of the possible methods and techniques
available for gray zone actors. I have carried out a small-scale content analysis
of Hungarian online media in order to illustrate a rather interesting phenom-

---

34   It is not my intention to examine actual, day-to-day issues of Hungarian domestic or foreign
        politics. This case study is included here only because it is accessible to empirical research.

enon related to information warfare – a characteristic feature or element of gray zone activities.

The time period of the investigation is from 2015.01.28. to 2017.05.02. An overall number of 67 articles were examined, published by either one of the two major Hungarian news portals on the internet. A kind of snowball sampling method was applied: at the first step I searched for an expression considered to be relevant and then I collected and organized the list of results (articles) into a standardized database. At the second step I simultaneously gathered the necessary information to be analysed by opening the articles individually and (at the same time) registered those articles in the sample database which have been offered by the webpage of the online news portal as ones might be interesting for me as a reader of the actual article. These two steps have been repeated several times, resulting in the 67 articles. The sampling method is not meant to, and does not, lead to statistically representative observations, but rather an explorative and indicative picture can be drawn. I applied an approach of studying the *labels* and *keywords* (113 in total) that were associated with, and linked to, the articles by the authors/editors as expressions representing the main content elements of the article. In this way it is more efficient to explore how the issues are thematized in (this segment) of public media and an overall picture can be drawn by mapping the pattern of connectedness between issues and topics. In order to explore the relations between single labels and keywords or amongst the groups of labels and keywords I applied standard network analysis methods.

According to the composition of the thematic labels in the online discourse the threat of certain countries (including Hungary) being attacked in the virtual domains seems to be publicly stated and acknowledged. Some articles address the information aspect of gray zone activities raising the public awareness about the challenge and unveil this tactic and method of hybrid aggression. That is, the threat is reflected in the public discourse enabling the society to become more conscious about the gray zone phenomenon itself (*'whitening' gray zone*). However, it is even more interesting how the expressions that make hybrid actions more visible for the public are connected. The two labels of *'hybrid threats'* and *'information war'* (figure 5.) prove to be linked to different keywords creating seemingly two separate partitions (*'cyber-defense research center'*, *'disinformation'*; *'Tech'* and *'domestic'' Ukrainian crisis'* respectively). The thematic element linking these quasi different sections is *'Russian propaganda'*. That is, the issue of information warfare and hybrid methods of war prove to be represented in the focus of activities attributed to Russia.
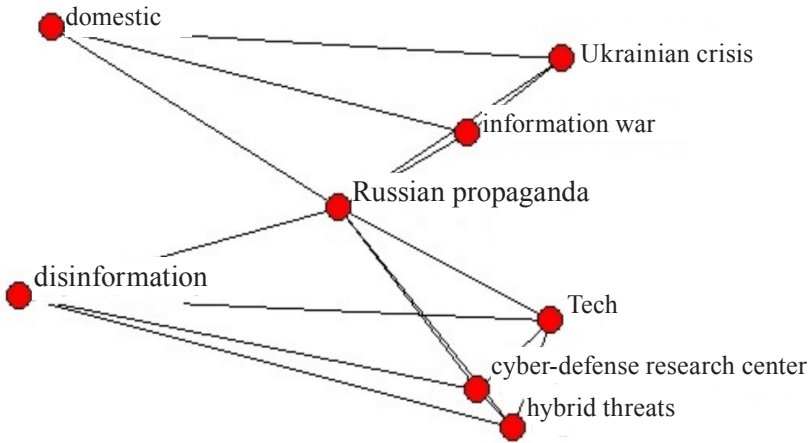
Figure 5.
Representation of hybrid threat in the online media

SOURCE: calculations by the author based on complex dataset

The label '*Russian propaganda*' itself however implies a conceptual network (figure 6.) which incorporates a wide range of themes: the connections among the labels and keywords evolves into a far-reaching context with topics of *corruption*, *foreign policy*, *home affairs* and *extremists*.
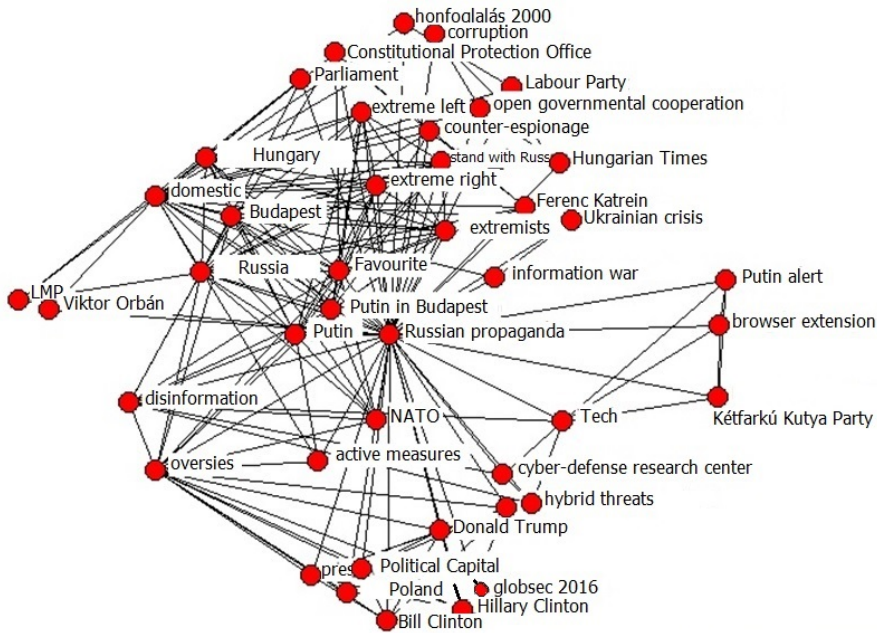
Figure 6.
Labels and keywords interconnected around 'Russian propaganda'

The presence of the label '*domestic*' reflects that the public representation of this hybrid threat associated with the Russian propaganda is relevant (also) from the perspectives of home affairs, which highlights the interdependence between the gray zone activity initiated from abroad and the consequences emerging in the indigenous sector. Notwithstanding, the other node on the left part of the network might raise more attention as '*disinformation*' both supplements and enriches the former thematic representation. If the labels and keywords connected to '*disinformation*' are also included, the result is a more detailed structure of the same topic (indicated by the expressions of '*Russia,*' '*Putin,*' '*NATO*'), and, on the other hand, additional aspects or themes appear. Namely the keyword '*disinformation*' paves the way for the appearance of the – strictly speaking – unrelated labels signifying the *Central European University* and *migration* (figure 7.).
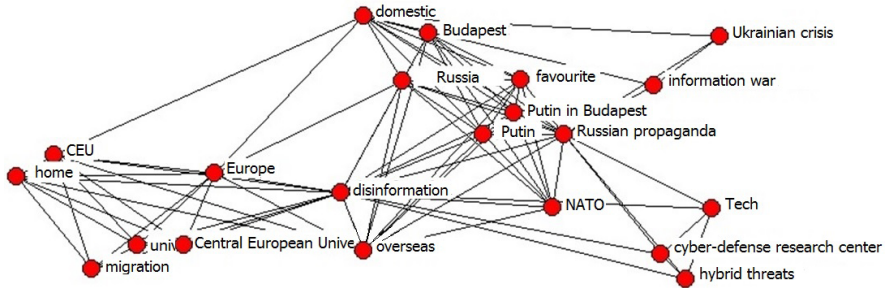
Figure 7.
Labels and keywords interconnected around 'disinformation'

SOURCE: calculations by the author based on complex dataset

The expansion of the conceptual network in this seemingly strange direction might be explained by the practice that in public discourse certain, initially unrelated issues are expressed, argued and interpreted by using some elements of the characteristic terminology linked to hybrid attacks or gray zone activities. This trend seems to be even more corroborated if the conceptual network gets expanded even further: it becomes clearly visible that the topics of '*hybrid threats*' (along with the keywords of '*cyber-defense research center*', '*Russian propaganda*'), '*refugee/migrant crisis*' (represented by – for example the – labels of '*refugee*', '*migrant*', '*Syria*', '*Islamic State*', '*Bashar el-Assad*') and '*civil organizations*' (represented by – for example the – labels of *'Hungarian Helsinki Committee', 'Hungarian Civil Liberties Union', 'Soros Foundation'*) are connected by the keyword '*disinformation*' which plays the key intermediary role. Social-political affiliation of the news portals emerges as a further distinctive dimension, as the arrangement of the network (figure 8.) makes is possible to separate the labels and keywords belonging to articles published by the online portals occupying various points of the political spectrum. The labels and keywords affiliated with the various socio-political approaches are segmented horizontally in the network structure, however, it should be noted that this arrangement is not due to an artificial intervention, rather it emerges from the pattern how the different expressions are connected with each other. This arrangement pattern might imply that the various social-political sides seem to utilize the notions and expressions linked to gray zone or hybrid activities to a certain extent, although they thematize in this way different issues and topics.
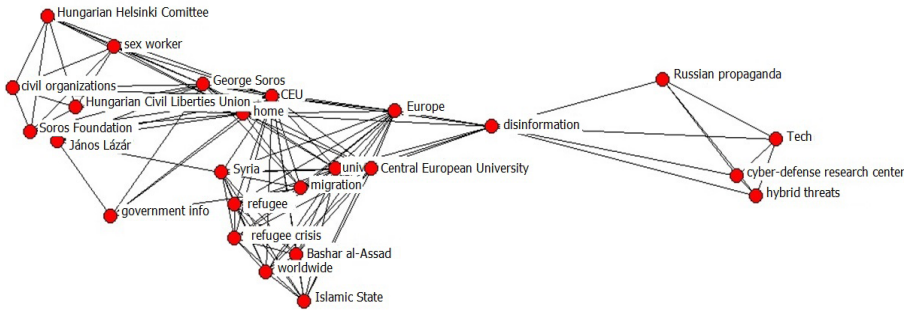
Figure 8.
Topics connected through 'disinformation'

Source: calculations by the author based on complex dataset

Based on the – primarily illustrative, rather than representative – results of this small-scale content analysis of articles from Hungarian online news portals it can be said that the gray zone or hybrid conflict phenomenon – or at least certain aspects of it – seems to be addressed in the public discourse. Ideas, methods, concepts (e. g. hybrid threats, information warfare, disinformation) have entered public discourse, which might be interpreted as a favourable outcome, as it could contribute to society's ability to cope with the challenge. On the other hand it might also be noted that this publicity is embedded in a divided socio-political context, and that the issue of hybrid or gray zone conflict could inevitably be exploited to satisfy short-term political interests.

A fragmented civil sector[35]

A similarly politically embedded topic is the subject of the last case study: I have investigated – initially – the financing network of the civil sector in Hungary. The primary objectives of this case study are to explore the map of connections and the pattern of integration between the civil organizations and funding institutions originating from the granted projects and to reveal if any differences in composition or distribution of the grants can be measured.

In order to be able to empirically investigate the financing network of the civil organizations in Hungary I built a complex database compiled from a publicly accessible register of the various funding institutions. On the one

---

35   As stated earlier, it is not my intention to examine actual, day-to-day issues of Hungarian domestic politics. This case study is included here only because it is accessible to empirical research.

hand I have made an approximately ten percent random sample of the projects of the Hungarian civil development fund, and from this sample I made an estimation about the share and number of successful (i.e. funded) projects. I complemented this database with the list and funding information of the civil organizations having granted projects financed by other supporters. In this phase data from two foreign granting institutions were added to the Hungarian sample. This way I created a database of the financing network of the civil organizations, which contains data on 5197 projects of 5058 civil organizations with one domestic and two foreign funding institutions. The database covers the year 2015, for which common funding information was easily accessible from public sources on the internet. In the course of data analysis I applied standard descriptive statistical and network analysis methods.

The main findings reveal a fragmented, but integrated structure: the organizations and the funding institutions are linked through the multiple relations of their several funded organizations. The civil network is overwhelmingly dominated in numbers by the organizations that have granted projects by the domestic funding institution. Only a significantly smaller fraction of the civil sector consists of the civil organizations funded by institutions operating abroad. Furthermore, it can also be observed that the different foreign founding institutions have partially supported civil organizations that have also had successful projects in the dominant domestic granting program. A small group of civil organizations that have granted projects from both of the foreign funding institutions can also be shown, and there is the further rather important fraction of civil organizations which are connected to all of the three funding institutions and in this way having the essential role of directly linking them and realizing the overall integration of the civil sector (figure 9.)
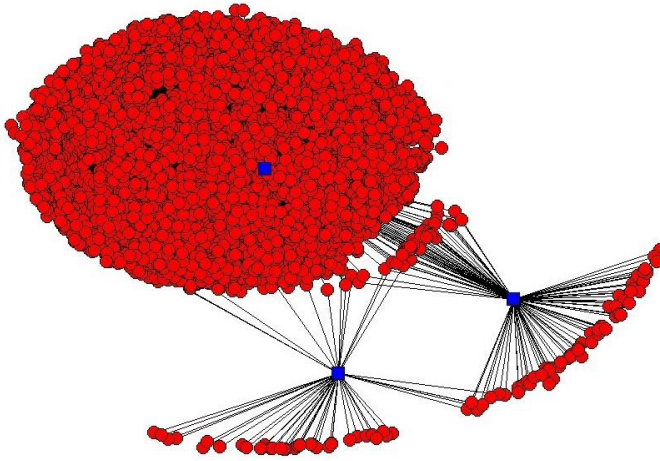
Figure 9.
The financing network of the civil sector

In the remaining part of this analysis I had to restrict the investigation to those organizations that had projects funded by more than one funding institution. This limitation was necessary partly due to the lack of accessible data, and partly to the excessive burden of collecting such data as were available and keying them in item by item to create the database. This sub-graph of the complete network consists of 150 organizations and data about 206 funded projects. Considering these limitations, the following results of this analysis need to be treated only as informative or illustrative, and should not be generalized for the total population of the civil sector.

Considering the composition of the civil organizations linked to the various funding institutions, some moderate differences can be measured.[36] The share of the civil organizations registered with headquarters in Budapest varies among the funding institutions. While the overall mean value for the Budapest based civil organisations is 56,3 percent, one of the foreign funding

---

36   In the further part of this analysis it is necessary to limit the investigation – due to the lack of accessible data and of capacities to one by one collect and assemble in a database – to the fraction of the organizations that have financed projects from more than one funding institution. This sub-graph of the complete network consists of 150 organizations and data about 206 funded projects. Considering these limitations the following results of this analysis need to be treated only as informative or illustrative and might not be generalized on the total population of civil sector.

institutions funds Budapest based organizations at a significantly higher rate (81,3 percent). Another dimension along which the distribution of the civil organizations seems to show a noteworthy difference is the rate of the granted organizations not registered officially as a civil organization in the Hungarian registry.[37] Approximately one-tenth (9 percent) of the organisations are in the unregistered category, and their share differs among the funding institutions. As one of them – the same one that showed a higher share of the Budapest-based organizations – can be characterised by a remarkably higher rate (23,4 percent) of unregistered organizations. Financial resources distributed to the organizations through granted projects also seem to show certain differences: comparing to the average (12,2 million HUF) of the grant per project values – computed at the organizational level – the aggregated data is lower in the cases of all funding institutions,[38] however a remarkable inequality can be measured in the distribution of the average budget of the projects among the granters. Remarkably lower amounts are allocated by the domestic funding institution (200 000 HUF on average) on a single project compared to other granters (table 2.).

civil organizations financed by… institution	Share of Budapest-based organizations (%)	Share of unregistered organizations (%)	Average budget of funded projects (million HUF)
foreign (1)	54,6	5,7	4,3
domestic	41,8	3,1	0,2
foreign (2)	81,3	23,4	7,7
mean	56,3	9,0	12,2

Table 2.

Differences in the financing of civil organizations

SOURCE: calculations by the author based on complex dataset

---

37   As a part of e-government services, information on the Hungarian civil sector can be found on the internet on an interactive webpage (www.birosag.hu), containing search options in the list of civil organizations. I used this list to update the database with the information that a particular organization could not be found in the registration list. This variable may be treated as an indicative one regarding the official status of the organization, however it must also be noted that some civil organizations may neglect to carry out the registration procedure and in this regard (also) the data gained from this source can be – distorted to a certain extent.

38   This can be explained by the great – rather much greater – differences of fund absorption capacity among the single civil organizations.

So the –informative, rather than representative – pattern of differences among the funding institutions implies that in the case of the domestic funding institution a lower share of Budapest-based organizations, a lower rate of unregistered organizations, and the lowest value of grant distribution capacity can be observed. It should be considered that – obviously – there is a great disparity in the numbers of civil organizations funded by the particular institutions, therefore they must follow fundamentally different funding policies. Due to the numerous applicants, the domestic funding institution might not apply the supporting process – featuring better targeting, more concentrated fund allocation – that the foreign granters follow. This – at least partially – explains the differences introduced above.

A rather one-sided and simplified, vaguely communicated interpretation of the financing network – described systematically above – emerged in the public discourse, again utilizing specific political interest. In turn, the other pole of the political sphere has also recognized a fragment of the Hungarian civil sector – one that includes formal organizations, bottom-up communities, social movements and even extremist groups which are – considered to be – supported by political parties. It is also acknowledged that this politically promoted segment of the civil sphere represents and cultivates specific culture and values – adequate and favourable for their advocates.
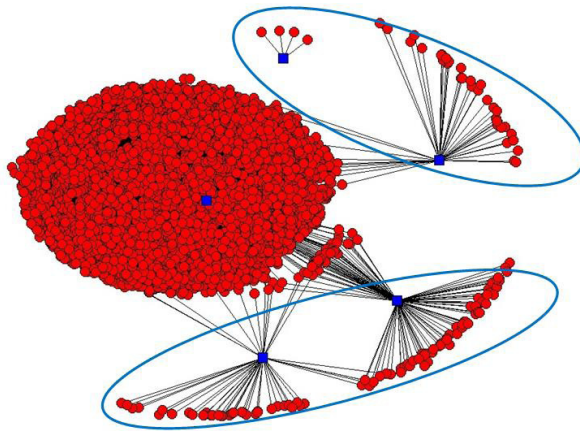
Figure 10.
A partially polarized pattern in the civil sector

Source: calculations by the author based on complex dataset

Considering these arguments, the empirical description of the civil sector outlined above can be improved by complementing the organizations supposed to be belonging to this opposite political section. I assembled and included in the network database the ones I could find sufficient information on. Their inclusion in the database resulted in a graph that represents a partially polarized arrangement (figure 10.). One of the new political supporting institutions exhibits similar pattern to those described earlier: there are civil organizations that are linked only to this institution, but it can also be stated that there some other organizations are connected to the domestic funding institution as well. The other new – rather small – fraction being formed around the other political supporting institution is completely isolated.

Due to the lack of accessible data the trends of the financial patterns cannot be investigated in the case of these new actors of the civil network, unlike the other two dimensions. There can be measured a rather high rate of Budapest-based organizations and a similarly great – actually the greatest – proportion of unregistered organizations among the civil and other bottom-up groups thatt are (considered to be) connected to and promoted by political parties (table 3.)[39].

civil organizations promoted by... institution	Share of Budapest-based organizations (%)	Share of unregistered organizations (%)
foreign (1)	54,6	5,7
domestic	41,8	3,1
foreign (2)	81,3	23,4
political party (1)	72,5	25,6
political party (2)	100,0*	75,0**
mean	56,3	9,0

Table 3.
Differences of the civil organizations in the extended network
* (n=1) ** (n=4)
Source: calculations by the author based on complex dataset

So according to the – dominantly illustrative – final outcome of this empirical case study the a conclusion can be drawn that the rather complex

---

39   Although in the case of political party (2) the overall number of observations is very few so this should be treated only as a rather informative data.

Hungarian civil sector can be considered to be moderately fragmented; partially polarized by different financing institutions and supporting parties that represent and cultivate opposing values, objectives and cultural orientations. A rather outstanding similarity between the two opposing poles regarding the composition of the civil organizations linked to them is the remarkably high rate of Budapest-based and unregistered organizations.

CLOSING REMARKS – A CHALLENGE TO ADAPT (?)

Ambiguity is an essential element of gray zone conflicts, as it can be known from the scientific literature and as it has been empirically illustrated and analytically described in the case studies introduced in this paper. It obviously emerges as a great challenge of trust and undermines cooperative intentions on a strategic level if certain actors in a multi-player interaction assist and at the same time violate the purpose of the overall initiation or the interests of (some of the) partners involved, as it was demonstrated in the first case study revealing the ambiguous structure of the international cooperation network to fight global terrorism, including the great gray zone actors in a 'friend and foe' situation.

Gray zone challenges and hybrid threats connected to the media, information warfare and propaganda can be tackled if the narrative of the adversary is successfully discredited and the division in the public discourse is mitigated by legitimate and fact-based information.[40] In this sense the findings of the second case study – revealing the division of public discourse in online media concerning the hybrid threat itself – might prove to be considerable. In an extremely divided information medium it cannot be convincingly expected that the recipients of the narratives can build a proper notion about hybrid conflicts and the potential risks they induce. It is dominantly the responsibility of those sources and communicators which present or strengthen an inappropriate – either over-, or underemphasized – impression of information warfare and propaganda in favour of their short-term political interest as these practices increase uncertainty and contribute to the deepening of the division.

Civil society groups can have an essential role in the process of coping with or repelling hybrid threats by adding credibility to the defensive initiatives

---

40   The Gray Zone: 7.

aimed to overcome deceptive propaganda and misinformation[41] – unless the civil sector itself is divided and polarized – as the third case study illustrated. If it becomes relevant to consider that the essential and unique elements of society, the civil organizations act on behalf of special interests – either linked to foreign groups or domestic political formations –, it easily can erode the trust and integrity of society and could leave it unprotected against truly serious interventions.

It seems to be an admissible conclusion that any initiation aimed to adapt the challenge of gray zone activities and hybrid threats should primarily consider to terminate or to diminish ambiguity. Which necessitate and involve methods to prevent from emerging and escalating those activities and mechanisms – at least partially illustrated empirically in this paper – which may lead to division and uncertainty. In a complex society this may prove to be a rather significant challenge.

PETER BALOGH (1982.) studied sociology at the University of Szeged. After graduation in 2006 he became a PhD-student of economic sociology at the Institute of Sociology and Social Policy of the Corvinus University in Budapest, where he earned his PhD degree in 2012. Subsequently his scientific interest turned toward new topics: organized crime, securitization, asymmetric warfare and hybrid war. He carried out quantitative research on the negative effects of social capital, exploring the global cooperative network of terrorist organizations. Currently he is investigating the social dimensions of contemporary warfare. He works as an assistant professor at the University of Szeged, Department of Sociology. He can be reached at: baloghp@socio.u-szeged.hu.

BIBLIOGRAPHY

BRANDS, H. "*Paradoxes of the Gray Zone*". Foreign Policy Research
        Institute. 2016 – http://www.fpri.org/article/2016/02/paradoxes-gray-zone/
FREIER, N. P. (ed.) *Outplayed: Regaining Strategic Initiative in the Gray
        Zone*, A Report Sponsored by the Army Capabilities Integration

---

41   BRANDS. "Paradoxes of the Gray Zone." 5.

Center in Coordination with Joint Staff J-39/Strategic Multi-Layer Assessment Branch. Strategic Studies Institute, U. S. Army War College Press. 2016; 64–70., – https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325

GHEMAWAT. P. ALTMAN, S.A. "*DHL Global Connectedness Index 2016*" Deutsche Post DHL, November 2016. – http://www.dhl.com/en/about_us/logistics_insights/studies_research/global_connectedness_index/global_connectedness_index.html#.VFff5MkpXuM

HLATKY, S. v. "*NATO's Public Diplomacy in the Grey Zone of Conflict*" USC Center on Public Diplomacy. 2016 – https://uscpublicdiplomacy.org/blog/nato%E2%80%99s-public-diplomacy-grey-zone-conflict

LIANG, Q., XIANGSUI, W. *Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House*, 1999 – http://www.c4i.org/unrestricted.pdf

OBERNIER, J. A., SANDERS, F. A. "*Enabling Unconventional Warfare to Address Grey Zone Conflicts*". Small Wars Journal 9. 2016 – http://smallwarsjournal.com/jrnl/art/enabling-unconventional-warfare-to-address-grey-zone-conflicts

OSKARSSON, K. "*The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone*" OPEN Publications 1/2. 2017; 1–16. – https://www.openpublications.org/single-post/2014/05/01/The-Effectiveness-of-DIMEFIL-Instruments-of-Power-in-the-Gray-Zone
"*Report on Gray Zone Conflict*" International Security Advisory Board. U.S. Department of the State. 2017 – https://www.state.gov/t/avc/isab/266650.htm

The Gray Zone. United States Special Operations Command White Paper. Public Intelligence. 2015 – https://publicintelligence.net/ussocom-gray-zones

VOTEL, J. L., CLEVELAND, Ch. T., CONNETT, Ch. T., IRWIN, W. "*Unconventional Warfare in the Gray Zone*" JFQ 80/1, 2016; 101–109. – http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.

LAZAR BERMAN and YANIV FRIEDMAN

The Suppressed Sword: Legitimacy Challenges in Gray Zone Conflict

(Israel, Dado Center for Interdisciplinary Military Studies)

ABSTRACT: In the national security realm contemporary concepts and assumptions face increasing irrelevance when they meet reality on the battlefield. As a consequence powerful states frequently fail to respond effectively to persistent and dangerous adversaries, who found a way to counteract Western military advantages, and to render them largely irrelevant. The word that surfaces repeatedly in the literature is "ambiguity." The term's frequency reveals a lack of confidence in defining the challenge and applying clear concepts to it. A lot of thinking and knowledge development must be done in order to come up with relevant concepts and doctrine to face the problem. This paper seeks to address this issue. It intends to apply rigorous theoretical thinking about gray zone conflict that is also useful to military leaders. It will explore the challenges of legitimacy in gray zone conflict, and will offer approaches for addressing those challenges.

INTRODUCTION

In recent decades, Western powers have struggled to make sense of the world around them. This is especially true in the national security realm, where contemporary concepts and assumptions face increasing irrelevance when they meet reality on the battlefield. This is no mere rhetorical problem. It has real world consequences, as ostensibly powerful states fail to respond effectively to persistent and dangerous adversaries.

The "gray zone" idea is an attempt to bring Western military thought in line with challenges these countries are already facing without adequate concepts and tools. While competition in the space between war and peace is certainly not new, the term itself has gained prominence as an uneasy understanding sets in that we face something that does not fit into our current conceptual and

operational toolkit. Our adversaries have found a way to counteract Western military advantages, and to render them largely irrelevant. Iran, Russia, and China all present complex challenges in a potential future conflict, and few in the West are confident that they possess the concepts and ideas to emerge the decisive victor.

The word that surfaces repeatedly in the literature is ambiguity. But the challenge is not inherently more ambiguous than other types of competition. Instead, the term's frequency reveals our own lack of confidence in defining the challenge and applying clear concepts to it. It is easier, it seems, to label the problem "ambiguous" and not perform the challenging and often frustrating task of defining the challenge accurately. Indeed, there is much thinking and knowledge development that needs to be done in order to come up with relevant concepts and doctrine to face the problem.

Israel- and to a significant extent the United States and other Western powers- struggles to use its considerable military might against weaker actors because it lacks the international and internal legitimacy to do so. Gray zone conflict presents even more challenges around legitimacy because of the difficulties of assigning responsibility for hostile acts, and the non-military nature of much of the activity. In addition, there is a perception that the challenge demands a law enforcement response, rendering the use of military might against attacks typical of gray zone conflict extremely problematic. We have not seen any discussion of this issue in the literature, and we see this as a problem that can potentially stand between success and failure if not studied and prepared for properly.

Despite ongoing legitimacy challenges, Israel has found certain ways to deal with new, potent threats without resorting to conventional warfare in the past, and continues to do so today. Sometimes it responds with traditional military tools, sometimes with other tools of national power.

This paper will explore the unique challenges associated with legitimacy – and by extension deterrence- in gray zone conflict. It will then look to the Israeli experience in order to provide operational, conceptual, and force design recommendations for Western powers confronting enemies that operate in the gray zone.

This study takes two important theoretical discussions and combines them to address the issue. It will first discuss Israel's legitimacy challenge in general, and will examine it more deeply through several case studies. It will then combine this insight with theory on the gray zone in order to come to an

understanding of the unique challenges around legitimacy brought about by gray zone conflict.

DEFINITIONS

Unfortunately, there is significant confusion and disagreement over basic concepts around gray zone warfare, including around core definitions. These definitions are crucial to any focused treatment of this issue. But authors have been inconsistent and untidy with their definitions. Many articles on gray zone conflict tend to conflate gray zone warfare with other types of unconventional conflict, especially with hybrid warfare. "Monikers such as irregular warfare, low-intensity conflict, asymmetric warfare, Military Operations Other Than War (MOOTW), and Small Wars have all been employed to describe this phenomenon in the past," reads the United States Special Operations Command White Paper "The Gray Zone."[1] NATO's OPEN publications study," The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone" explicitly equates hybrid and gray zone warfare. "Hybrid conflict, also called 'Gray Zone' conflict, lies between 'classic' war and peace…" the study reads.[2] If it just the latest trendy name for a problem we were discussing five or ten years ago, there is no reason to invest significant resources in thinking about an old problem with a new name.

The authors posit that gray zone warfare is distinct in meaningful ways from other types of subconventional warfare, including hybrid warfare. Hybrid warfare, for instance, uses conventional and other means, including terror, guerilla warfare, civilians, and more within the same battlespace. It is clearly war. An especially problematic aspect of gray zone strategies is that they remain below the threshold of conventional conflict. Though it is not a new phenomenon in history, it still demands it own analysis and discussion, of which this study is one piece.

This work uses the following definition:
A strategy by which an actor attempts to change the status quo through means short of conventional military methods, in order to achieve goals

---

1   The Gray Zone. White Paper, United States Special Operations Command. September 9, 2015.
2   OSKARSSON, Katerina. «The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone.» NATO Open Publications, Winter 2017.

typically gained through conventional campaigns. This gradual strategy is chosen in order to avoid provoking a way in the gray zone actor would be at a disadvantage.

An example of a goal referenced above is capturing territory. Traditionally, territory is seized by conventional methods, especially ground maneuver. But Russia and China have both seized territory without resorting to such means.

THE CHALLENGE FOR ISRAEL

The gray zone strategy is uniquely problematic for Israel. This challenge can be illustrated through an examination of Israel's National Security Concept as it meets a gray zone strategy.

The National Security Concept has three plus one pillars: Deterrence, Early Warning, and Operational Decision, plus Defense, a recent addition. A gray zone strategy is problematic for each one of these pillars.

Israel is a small country, in terms of both population and territory. As such, it seeks to maintain the status quo and avoid war. When fighting does occur, it must win quickly, as it relies on its reserve force, meaning the economy grinds to a standstill as tens of thousands of working age men go off to fight. It must keep the fighting away from its population and industrial centers, which lie close to hostile borders.

Israel relies on its deterrence, which rests on its military might and past successes, to prevent war. Should deterrence fail, it relies on capable and advanced intelligence services to provide an early warning of potential war, to give the country time to use diplomacy to prevent war, or to call up the reserve army that represents its maneuver force.

Should war break out in the end, Israel classically has tried to gain a speedy operational decision, using its reserve formations to take the fighting to enemy territory through dominant ground maneuver. This shortens the war and moves the fighting off of Israeli territory.

In recent years, a fourth pillar has been added, that of defense. In times of war, defense improves Israel's ability to move the fighting to enemy territory, and improves Israel's deterrence – after all, if enemies understand they cannot harm Israel's homefront, why pay the price of war?
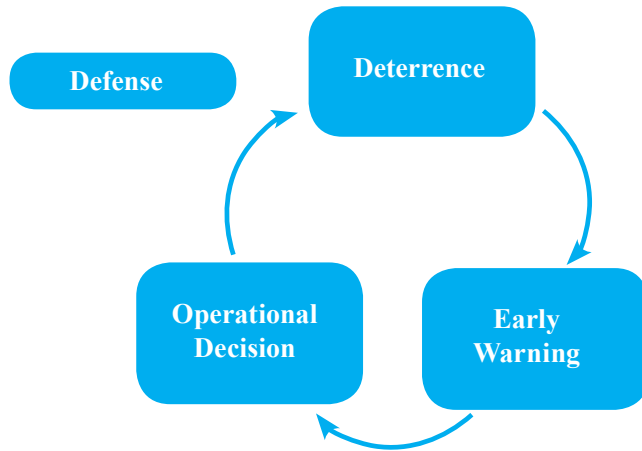
Figure 1.
The four pillars of Israel's National Security Concept

But gray zone strategies challenge every single one of these pillars. Gray zone strategies are meant to stay just below the red line that a country protects through deterrence, and eventually erode those red lines, damaging deterrence.

Moreover, the gradual gray zone strategy, over many years, is not the kind of threat that the early warning system is designed to identify.

There is often no clear military force to defeat on the battlefield. The mix of locals, militias, cyber, propaganda, etc, is not a challenge our maneuver forces are designed to defeat on the battlefield.

And Israel's defense is largely geared to protect against kinetic threats (and cyber) and not gradual campaigns like gray zone strategies. As such, gray zone strategies are especially problematic for Israel and its classic security concept.

Though Israel has its own unique set of challenges when facing a gray zone strategy, it also faces the same overall problem as other conventional militaries. Though gray zone challenges are not only a military problem, the military is unquestionably one of the key actors, and plays a role in potential solutions.

The broad military problem revolves around red lines. Gray zone actors seek to avoid military conflict – in which they see themselves at a disadvantage – and thus are careful not to cross our red lines. However, they do carry out actions that fall just short of triggering our military response. Over time, they even succeed in pushing those red lines further back by identifying and exploiting the areas we ultimately fail to defend, eroding our deterrence and credibility.

Though gray zone strategies seek to remain below the threshold of conventional conflict, they do not do so indefinitely. By gradually eroding red lines, damaging our credibility, and calling into question alliances and policies, a gray zone actor positions himself to be at an advantage if conventional conflict does indeed occur. By taking control of islands in the South China Sea, China is in a better position should it be forced to deny access to a Western invading force, and it has created dilemmas for the US-led alliance system in the process.

Another ongoing challenge conventional militaries face is in force design. Our militaries are structured around services that correspond to domains – land, air, sea, and soon space. Each is organized around certain groups of challenges. But the challenges in a gray zone conflict – restive local populations, propaganda, militias, "private" companies – don't fit into our service model. All of our effort creating exceptional services to handle problems in their domains does not meet the problem created by gray zone actors.

The exception in this case if the cyber threat, an important component of gray zone strategies, especially that of Russia. Conventional militaries have begun to create significant organizations to meet the cyber challenge. The United States created the Cyber Command within its Strategic command in 2009, and Israel decided to boost its cyber defense unit into an operational command within the Computer Service Directorate.

LEGITIMACY

What do we mean by the term "legitimacy?"
In this context, legitimacy refers to the authority in the eyes of others to exercise power, in this case, military force.

There is more than one type of legitimacy, and a country can have one type without the others. Fundamental legitimacy is the right to exist, meaning the right to use military force in self-defense in general. This is long-term strategic legitimacy.

Moving down a level, there is legitimacy to engage in a specific military campaign – Lebanon in 2006, for instance, or an operation against Hamas in Gaza. One could think that could that a country has a legitimate right to self-defense, but could claim it has no right to pursue a particular campaign. This is somewhat parallel to jus ad bellum from the world of military ethics, the moral right to engage in a particular war.

In legitimacy, as in the ethics of war, even if you have the standing to engage in the campaign, that does not mean that every action within that campaign has legitimacy. There is situational legitimacy, in which certain tactics and munitions might be seen as illegitimate, in the midst of a campaign that does enjoy legitimacy.

It is important to note that "legal" and "legitimate" are not identical, although there is significant overlap. Still, the world of legal military actions is generally much larger than that of the legitimate. There are numerous legal military capabilities and activities that a Western military could use, but chooses not to because it lacks the legitimacy to do so. For example, white phosphorus is illegal to use against personnel, but is entirely legal to use as a smokescreen to mask military movements. Some militaries have chosen to refrain from even legal uses of white phosphorus because of legitimacy challenges. For instance, after Operation Cast Lead in Gaza in 2008/9, the IDF deputy chief of staff said that the "big buzz in the media" – not legal issues – led to an order during the operation to stop using such munitions. "These shells were used only to create smokescreens, in keeping with international law," he emphasized.[3] At the same time, there are even some cases where something is seen as legitimate but is not legal.

One might think that this is only a problem for the spokesmen and public relations staff. Why should the IDF care whether other think it is justified in using military force?

Legitimacy challenges have a clear effect on the military. Though the IDF is an extremely capable and advanced organization, it loses the ability to use many of the important tools at its disposal when it lacks legitimacy to do so. This obviously has a direct effect on the course and outcome of campaigns, on the safety of soldiers and civilians, and much more.

A lack of legitimacy – or an anticipated lack – also has the effect of deterring Israel at all levels of war, strategic, operational, and tactical. It has been forced to change its preferred course of action because of legitimacy problems. Of course, like any deterrent, if the interests are great enough, Israel will act regardless, but it is certainly a consideration at all levels of Israeli planning.

---

3   FRENKEL, Sheera. «Israel backs down over white phosphorus.» The Times, April 23. 2009.

Israel's legitimacy challenges

Israel's freedom of action can be significantly constrained by legitimacy challenges. This work will present three examples in which Israeli tactics, operations, and strategy were forced to change because of a lack of legitimacy.

In June 2006, IDF corporal Gilad Shalit was kidnapped by Hamas terrorists inside of Israel's border with Gaza. Two week later, Hezbollah attacked an IDF convoy inside Israel's border with Lebanon, killing three and kidnapping two reservists. In response to both incidents, Israel wanted to strike at mixed-use civilian-military infrastructure in order to pressure Hamas in Gaza and Hezbollah in Lebanon to return the soldiers.

In Gaza, Israeli planes struck an electricity plant. The Bush Administration, however, would not accept the damage to Gaza's infrastructure, and pressured Israel to stop, which it did.

In Lebanon, Israel went into the war intending to embark on a campaign with a similar logic. But the campaign in Gaza, along with American concern for the stability of the government in Lebanon, led the Bush Administration to oppose strikes on mixed-use infrastructure from the start. Israel was forced to change the entire strategic logic of its campaign from pressuring the Lebanese government to one of harming Hezbollah's capabilities.

During the campaign against Hezbollah in 2006, legitimacy challenges had widespread effects at the operational level. Israel carried out an airstrike on buildings in the village of Qana from which Katyusha rockets were launched against the city of Haifa. Sometime after the strike, a building in Qana collapsed, killing 28 civilians in the rubble. Israel was roundly criticized by the international community for not doing more to avoid collateral damage, and in response to the outcry, Israel decided to halt most of its airstrikes for 48 hours. This move had obvious operational effects, as it released pressure on Hezbollah and gave the organization time to regroup.

Legitimacy challenges in gray zone conflicts

Having demonstrated the effects on all levels that legitimacy challenges have posed for Israel, this work will now examine how these problems could manifest themselves specifically in situations where a conventional Western military, like the IDF or US Armed Forces, face a gray zone challenger.

Legitimacy is especially tenuous in gray zone conflicts for several reasons. First, there is a challenge for the conventional military to identify the gray zone actor carrying out a campaign of seemingly uncoordinated actions, and then proving to both the world and to your own public that this actor is behind the hostile campaign. Without this proof, legitimacy to act, especially militarily, is hard to come by.

Second, the whole idea of gray zone strategies is built around avoiding the use of conventional force. But our militaries are heavily built around the use of conventional tools. It is always problematic to find legitimacy for the use of conventional forces challenges that are not conventional, and might not even seem military at all.

Third, we hope to prevent wars through deterrence. If an adversary crosses our red lines, he knows we will extract a cost that is too high for him. But gray zone strategies intentionally seek to remain just below our red lines, and to push our red lines back. The lack of legitimacy to act erodes our deterrence, emboldening our gray zone adversaries.

Fourth, many state actors rely on alliances in order to deter adversaries and defend themselves if deterrence fails. NATO is an especially important example of such an alliance. Allies are unlikely to agree to join a campaign against gray zone actors, who intentionally hide their activities and avoid open military actions. This alliance issue further weakens deterrence.

Fifth, our legal structures form an important source of legitimacy for military action. But the legal framework is designed primarily around conventional conflicts, and certainly around military conflicts. It is not designed to provide guidance for state actors against gray zone adversaries, and as such, it is harder to achieve legitimacy for military actions that do not have a clear legal framework.

Finally, legitimacy is an outcome of the war of narratives. Gray zone strategies are designed to erode the narrative of the state actor, damaging its legitimacy to act and use military force.

TOWARDS A SOLUTION

After having presented a worrying picture of the challenges of legitimacy in general and in gray zone conflicts in particular, this work will now turn toward possible approaches to address the challenge. First, it will present cases in which Israel succeeded in building legitimacy for military action,

outside of specifically gray zone campaigns. It will then apply those lessons to legitimacy challenges in gray zone conflicts.

Karine A

In 2002, Israel was in the midst of a multi-year terror campaign by a variety of Palestinian groups, including Islamist organizations like Hamas and secular ones like Tanzim. Israel was in search of a solution to the string of suicide bombings in its cities and shooting attacks on its roads. But as long as PA president Yasser Arafat was seen as a legitimate leader, Israel would not enjoy international support for a badly needed anti-terror military campaign, which would include measures like re-entering Palestinian cities.

Israel undertook three major lines of effort. First, it prepared its military for a complex operation against Palestinian terror. Second, it worked to build legitimacy among the Israeli public for the operation. Third, it worked to build legitimacy among European states and the US government for the operation. The second and third rested on finding evidence that Arafat was involved in the planning of terror.

The PA turned to Iran for weapons to use against Israel, while Iran was on the search for a foothold in the West Bank. On December 11, 2001, Israeli intelligence discovered a ship filled with Iranian military aid, the Karine A, sailing toward the Gaza Strip. In January 2002, Israeli commandoes intercepted the ship, and passed documents implicating Arafat to the Bush Administration. In addition, journalists were invited to document the captured weapons. The capture led to a change in the American attitude toward Arafat, and gave Israel legitimacy for a broad military campaign against Palestinian terror centers. Vice-President Dick Cheney was asked during an interview whether Arafat's role in the affair means he participated in a "terrorist mission", Cheney replied, "That's correct…In my mind and based on the intelligence we've seen, the people that were involved were so close to him it's hard to believe he wasn't."[4] President Bush himself was no less harsh: "I am disappointed in Yasser Arafat. He must make a full effort to rout out terror in the Middle East. Ordering up weapons that were intercepted on a boat headed for that part of the world is not part of fighting terror, that's enhancing terror. And obviously we're very disappointed in him."[5]

---

4   SATLOFF, Robert «The Peace Process at Sea,» National Interest, Spring 2002,
5   La GUARDIA, Anton. «Bush says Arafat is backing terrorism.» The Telegraph, January 26., 2002.

The Flotilla Challenge

As part of a campaign to break Israel's blockade on the Gaza Strip, or to force it into a costly mistake, the Free Gaza Movement organized a series of flotillas to Gaza starting in 2008. They carried nominal medical aid, but the real purpose was to either reach the Strip and weaken the blockade, opening the door for the unrestricted flow of goods- including weapons and terrorists into Gaza, or force Israel to stop them, embarrassing Israel on the international stage and possibly even removing the possibly of using force in the future.

In 2010, the Free Gaza Movement partnered with the Turkish Humanitarian Relief Foundation (IHH), which is banned in Israel and has been investigated for ties to terror groups in the West. It organized a flotilla of six ships that set sail on May 30, 2010. The following morning, IDF naval forces ordered the Mavi Marmara flagship to turn back. When it refused, Israeli naval commandoes boarded the ship. But a group of activists on the Mavi Marmara attacked the soldiers with knives, pipes, and possibly pistols. In the raging battle on board, nine Turks were killed and ten IDF commandoes injured.

International condemnation was swift and furious. "Let me be clear," thundered British Prime Minister David Cameron. "The Israeli attack on the Gaza flotilla was completely unacceptable."[6]

It appeared the activists had won an important victory, and the flotilla problem would only worsen for Israel, which could not risk being blamed again for the loss of life. But – surprisingly – Israel managed to put together a range of actions that caused the problem to dissipate. The next flotilla organized by the NGO in 2011 never even got out of port. Israel managed to create broad international opposition to the flotilla. Actors from the UN and the Quartet to Canada and France took public positions against the voyage. Even Turkey's foreign minister said that the organizers should reconsider, now that the Gaza- Egypt border was open. The Obama Administration reportedly ordered a Middle East peace conference in Ankara in exchange for its help in stopping flotilla.

Israel's quiet diplomacy had other effects. The Greek government, in whose ports most of the ships were docked, forbade them from setting sail for Gaza.

Israeli NGOs engaged in lawfare against the flotilla, warning maritime insurance companies that they could be held responsible for terrorist attacks that made use of any materials carried by the ships.

---

6   Berman, Lazar. «Bibi the Strategist.» Commentary, August 16., 2016.

They did the same for maritime communication companies whose services the flotilla needed in order to set sail. Israel NGO Shurat HaDin gave its account of its successful legal campaign against the flotilla: "Inmarsat, based in the UK and the US, is the main provider of maritime communication services, a crucial tool which enables vessels to reach their destinations. After sending a warning letter to Inmarsat for aiding and abetting terror organization, Shurat HaDin commenced a civil action against Inmarsat in Florida State Court on behalf of Michelle Fendel, a resident of the Southern Israeli town of Sderot. Among other things, the lawsuit sought a permanent injunction against Inmarsat which would require it to cease provision of all services to any Flotilla ship on the grounds that the provision of such services constituted aiding and abetting terrorism in violation of US law."[7]

By early July, most of the activists had simply given up and gone home. Israel easily intercepted the one solitary vessel that managed to sail toward Israeli waters, with no violence or international opprobrium. A subsequent flotilla attempt in 2015, with an Israeli parliamentarian and a past president of Tunisia onboard, was easily intercepted by Israel with no cost in blood or diplomatic standing. Israel even taunted the participants over megaphones, and prepared flyers reading, "Perhaps you meant to sail somewhere else nearby – Syria, where Assad's regime is massacring his people every day, with the support of the murderous Iranian regime."[8]

Through a broad, diverse campaign – diplomacy, lawfare, military force, and other actions – Israel recovered quickly from a mistake that seemed to imperil its legitimacy to act against flotillas. I managed to build up its legitimacy to prevent flotillas, and succeeded in stopping them in practice.

Iran in Lebanon

In Southern Lebanon in the 1990s, Israel faced a legitimacy problem. Since it was seen as an occupier, it had limited legitimacy to act against Hezbollah and its patron Iran. Iran provided weapons and military training to Hezbollah. This aid allowed Hezbollah to grow dramatically as a fighting organization. But it also helped Hezbollah carry out terror attacks inside of Israel and against international Jewish and Israeli targets, including the Jewish community center in Argentina and the Israeli embassy there. Israel understood that it

---

7   „Sinking the Gaza Flotilla." Shurat HaDin – Israel Law Center. 16. July 2016 – http://israellaw-center.org/campaigns/sinking-the-gaza-flotilla/
8   Berman. «Bibi the Strategist.»

still had legitimacy to act to stop terrorism, and therefore chose to focus on incriminating Iran in supporting Hezbollah terror. Iran understood that being seen as supporters of terror would create significant problems for them, and strived as best they could to keep their activities hidden.

The IDF caught Iran-trained Hezbollah operatives on the way to carry out an attack on civilian targets in Israel, and Israeli diplomats passed the information to their European and American counterparts. It showed Iran funding, training, and directing terrorist attacks. The incriminating evidence not only helped Israel in its diplomatic campaign against Iran, but also expanded its military freedom of action in Southern Lebanon against Hezbollah.[9]

A MODEL FOR A SOLUTION

The IDF experience suggests a possible model for dealing with legitimacy challenges specific to gray zone conflicts. Of course, there are many possible approaches to a solution, and this is one that the evidence in the Israeli experience points toward.

As we saw in the case of Yasser Arafat and Iran in Lebanon, incrimination is challenge and is of vital importance. Establishing the connection to hostile activities builds legitimacy for military escalation, if that is what we are seeking. At the same time, it creates urgency and purchase for your diplomatic efforts to counter the gray zone actor's hostile campaign. This is especially true if other countries are eager to prevent military escalation, and would prefer to support your diplomatic efforts instead.

---

9   BERGMAN, Ronen. The Point of No Return, Or-Yehuda: Kinneret, 2007; 159, 164, 198, 340, 349.
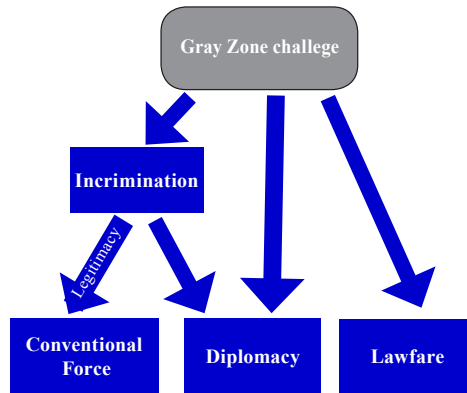
Figure 2.
Possible responses to Gray Zone challenges

Of course, diplomacy should begin even before the difficult process of incrimination comes to a head. Some process is possible, but skepticism is likely without proof of hostile actions by the gray zone challenger.

In dealing with a challenge that is not primarily military, the importance of lawfare emerges, as was seen the flotilla success. This can be undertaken by NGOs, governments, or cooperation between the two. This effort can create serious complex and unexpected problems for the adversary.

Other tools in the state toolbox can also be components of a campaign, the contours of which depend on the specific context.

CONCLUSION

From the combination of gray zone theory, past Israeli legitimacy challenges, and successful Israeli cases, a number of important conclusions come to the surface.

First, a gray zone strategy is a distinct strategy, and should be thought of separately from other unconventional strategies and types of warfare, including hybrid warfare.

Moving to legitimacy in general, in our modern era of YouTube, smartphones, and increasing sophistication of international and local organizations, legitimacy challenges will continue to grow for democratic states with conventional militaries. More military actions will be documented and scrutinized online, and NGOs will be better organized and equipped to pounce on alleged missteps.

Beyond broader legitimacy challenges, gray zone conflicts bring their own unique legitimacy challenges. Many of these are even more complex than in other contexts.

Still, there is hope. Looking at the past can offer approaches for dealing current and future threats. It is not enough to be reactionary. Just as we design military force and doctrine in order to meet terrorism challenges, cyber threats, and more, we must also create forces and doctrine to meet legitimacy challenges in the gray zone. Within this force, intelligence is crucial. Not only for early warning in terms of the threat itself, but also for incrimination and diplomatic efforts.

It appears that a new challenge has arrived. This challenge, gray zone strategies against conventional actors, will continue to confound leaders and planners for the foreseeable future. But if we learn from the past, understand the present, and anticipate the future, we can handle this problem as we have done with other complex challenges in the past.

LAZAR BERMAN holds an MA in Security Studies from Georgetown University. His thesis examined Israeli military innovation from 2000-2009. He was an editor at The Times of Israel, and taught at Salahuddin University in Erbil, Iraq. He previously served as an infantry officer in the IDF.

YANIV FRIEDMAN holds an MA in International Relations and History from Haifa University. His thesis examined Israel's security concept under Golda Meir. Friedman worked as a researcher in the National Security Studies Center at Haifa University, and is currently writing his doctoral dissertation at Tel Aviv University on the Eshkol Administration's security policies. He previously served as a reconnaissance squad commander in the IDF.

BIBLIOGRAPHY

BERGMAN, Ronen. *The Point of No Return,* Or-Yehuda: Kinneret, 2007; 159, 164, 198, 340, 349.
Berman, Lazar. "Bibi the Strategist." *Commentary,* August 16., 2016.
Berman. „Bibi the Strategist."

FRENKEL, Sheera. „Israel backs down over white phosphorus." *The Times*, April 23., 2009.

La GUARDIA, Anton. „Bush says Arafat is backing terrorism." *The Telegraph,* January 26., 2002.

OSKARSSON, Katerina. „The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone." NATO Open Publications, Winter 2017.

SATLOFF, Robert „The Peace Process at Sea," *National Interest,* Spring 2002,

„Sinking the Gaza Flotilla." Shurat HaDin – Israel Law Center. 16. July 2016 – http://israellawcenter.org/campaigns/sinking-the-gaza-flotilla/

The Gray Zone. White Paper, United States Special Operations Command. September 9., 2015.

Luís Manuel Brás Bernardino
Africa's Gray Zone: The Sahel

Abstract: Africa's Sahel region is one of the most complex, interconnected and challenging regions on the African continent. A huge region where some of the security problems that we are facing today in our globalized world are present creating one of the most relevant and complex grey zones in Africa and in the world. In this multi-faceted environment the major international security players are present and fight each day to contribute to a developed and safe region, where people can live and work in peace. One of the major players is the European Union, which, in accordance with the Sahel strategy, implemented the European Union Training Mission in Mali (EUTM Mali) in order to contribute to the development of the Malian Armed Forces as a strong contribution for the stabilization and security of the region.

Introduction

In the Sahel region extreme poverty, lack of regional economy, water problems, and climate change and particularly armed conflict and regional insecurity continue to threaten the lives of millions of people. These interdependent drivers are behind the staggering levels of structural, chronic and acute vulnerability present in the region. Where the chronic seasonal cycle is broken, progress and success can be seen. Where conflict hits, hard-won gains are quickly lost and new challenges appear.

Communities across the region remain highly vulnerable. In mid-2017, around 30 million people are expected to face food insecurity, and almost

12 million of them at crisis and emergency levels.[1] Pockets of pasture deficits have been observed in certain areas of Chad, Mali, Mauritania and Niger, and risks of locusts have been identified in Mauritania and neighboring areas.[2] The situation of people living in the conflict-affected regions of Mali and the Lake Chad Basin is particularly critical.

Crises and upheaval in the Maghreb and the Sahel have altered the regional security environment. Security challenges are increasingly becoming entwined, and many are becoming more pronounced amongst at-risk border communities in marginalized peripheries and rural communities. That's why we could talk about a "Gray Zone" and a "Gray Conflict" in the Sahel.

A DEFINITION FOR THE "GRAY ZONE"

We all know that the concept of "Gray Zone" conflicts are neither a situation of war nor a situation of peace, but instead it is somewhere in the middle. In fact, it is a mix of peace and war …a multi-faceted, complex environment where we have many actors and a huge variety of small powers competing together. Because of that complexity defining their characteristic is not an easy task – particularly if you talk about the main objectives, the participants (actors), and the international situation and also about the role that military forces should play in response.

They are consequently what we call a smart and comprehensive approach for some small rising powers, who wish to change the current international status to better serve their own interests and achieve their own goals. The main goal of a "Gray Zone" challenge is to achieve political-strategic gains, whether territorial, political, diplomatic or otherwise, and that are normally linked to a military triumph. However, "Gray Zone" is meant to achieve those gains without escalating to warfare, without crossing established international norms, and consequently without exposing the actors to the penalties and risks that such escalation might bring.

The term "Gray Zone" may be new but the phenomenon itself is not. Although many of the tactics, techniques and procedures (TTP's) used now are based on modern technology, notably cyber and networked communication,

---

1   Mali Central: La fabrique d'une insurrection? International Crisis Group, Rapport Afrique N° 238 – https://www.crisisgroup.org/fr/africa/west-africa/mali/central-mali-uprising-making

2   Mali Central: La fabrique d'une insurrection?

others are as old as the Vietnam or Korean Wars. What we now call "Gray Zone" methods and techniques have been employed in the past under such names as: "political warfare," "covert operations" and "irregular" or "guerrilla warfare." And the Portuguese Wars in Africa's old colonies in 1961-1974 are a very good example.

Gray, it seems, is neither white nor black. It suggests lack of definition, ambiguity, and also chaos and disorder. That is why the concept of "Gray Zone" conflict has recently generated significant attention and controversy in the military, political and academic world.

Perhaps the most widely used definition of "Gray Zone" conflict is that established by the U.S. Special Operations Command in 2015:

> *"...gray zone challenges are defined as competitive interaction among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks..."[3]*

I believe that a "Gray Zone" conflict is better understood as a complex political-military activity which is coercive and also violent, but which is also designed to remain below the level of a conventional military conflict or an open interstate war. It is usually a regional conflict between non-state actors but involving states. In some sense, in a "Gray Conflict" the instruments of a "Gray Zone" operation are used to create confusion and division in the "enemy mindset."

We are talking about infiltrating covert military forces, developing deception operations, and running covert operations in what we could call "enemy territory." The territory could be a country, an entire region or a huge part of a continent. Or it could be countries and regions on different continents, as we could see for example in the Sahel region. This territory could also be in the third dimension – the cyberspace.

---

3   The Gray Zone, U.S. Special Operations Command, September 9., 2015; p. 1. – https://info.publicintelligence.net/USSOCOM-GrayZones.pdf

A "Gray Conflict" in a "Gray Zone"

The principal characteristic of "Gray Zone" operations is that they employ methods that are outside normal international interactions, but without an explicit use of a military force. They occupy a gap between normal diplomacy, economical competition and sometimes open military conflict, while employing trade actions to deal with the "Gray Conflict" In one region.

"Gray Zone" attacks go beyond the typical forms of political and social interaction, and use military operations to make deliberate use of some instruments of violence. Additionally, they often involve asymmetric warfare, commensurate with national interests or national capabilities. It could also involve parts of a bigger zone where we concentrate the military initiative and focus our military, diplomatic and political activities. A "Gray Zone" could also be a huge area or region where neither the indigenous government nor the international community exercises control, and where a variety of state and non-state actors are vying for influence and power.

Contemporarily, "Gray Zone" challenges present special problems, in part because operations employ techniques to avoid confronting the military powers on grounds. Notably open conventional warfare, where military power, based on personnel, experience, technology, and economic capacity give big powers an edge. This makes "Gray Zone" acts difficult to comprehend in context until well after the transition to a conventional conflict has taken place.

These techniques, which may be broadly described as "asymmetric" include, among others:

- Employment of new technology - like cyberspace and social media;
- Use of weapons or tactics which the western countries, for legal and moral reasons, decline to use (for example the use of chemical agents);
- Operations in remote, unfamiliar areas, with different cultures, values, and an ability to reach traditionalist, nationalist, or religious groups (example: Sahel);
- Exploitation of differences between the big powers (countries or organizations) and their adversaries – normally small groups;
- Military intervention in contexts where there are no totally ideal partners and there is confusion about intentions, capabilities, and participants.

The "Gray Zone" diplomatic-military-operational techniques in a conflict may also include (either as a challenge, or as a response):

- Covert Operations under state or international organization control, espionage, infiltration, and sometimes subversion or state/regional political structures control;
- Cyber Warfare and control of the Cyberspace;
- Use of Special Operations Units and other state-controlled armed special units, and also other military personnel (according to the mission…);
- International support – logistical, political, and financial – to fight against insurgent, criminal organizations and terrorist movements;
- Economic pressures that go beyond normal economic regional competition;
- Recruitment of non-governmental actors, including organized criminal groups, terrorists, and extremist political, religious, and ethnic or sectarian organizations;
- Military Assistance to irregular military and paramilitary forces or national Armed Forces (this is what the EU is doing in the Sahel – EUTM Mali);[4]
- Reinforce or implement democratic institutions, including the electoral system and the judiciary system (this is also what the EU is doing in the Sahel – EUCAP Sahel)[5]

THE SAHEL AS A "GRAY ZONE"

Africa's Sahel region[6] is one of the most complex, interconnected and challenging region in the African continent. A huge region consisting of ten countries from the Atlantic Ocean to the Red Sea, where some of the security problems that we are facing today in our globalized world are present, creating one of the most relevant and complex Grey Zones in Africa and in the world. In this multi-faceted environment the major international security players are present and fight each day to contribute to a developed and safe region, where people can live and work in peace.

---

4   EU-Training Mission in Mali, – http://www.eutmmali.eu
5   EUCAP Sahel Niger. – https://eeas.europa.eu/csdp-missions-operations/eucap-sahel-niger_en
6   The Sahel is a semiarid region of western and north-central Africa extending from Senegal eastward to The Sudan. It forms a transitional zone – Border – between the arid Sahara (desert) to the north and the belt of humid savannas to the south. The Sahel goes from the Atlantic Ocean -Senegal, Mauritania, following the Niger River in Mali, Burkina Faso, Niger, Nigeria, Chad, and into The Sudan.

One of the major players in the region is the European Union, which, in accordance with the Sahel Strategy,[7] implemented the European Union Training Mission in Mali (EUTM Mali)[8] in order to contribute to the development of the Malian Armed Forces as a strong contribution for the stabilization and security of the region.

France's sudden military intervention in Mali in mid-2013 with Operation "SERVAL"[9] put the country's crises at the top of the international agenda. Since then the International Community has increased the military participation in the Sahel region and particularly in Mali. The Sahel has become, in my opinion, a special "Gray Zone" and the conflict involving many actors in the region has become a "Gray Conflict" for the entire world.

A scenario where a coalition of Tuareg nationalists defending the "AZAWAD"[10] independence, Islamic militias and various transnational criminal networks have split the country in half. With a military-led coup the government in Bamako in mid-2012 looks unable to lead a decisive response and find the right way to improve the peace and the development in the north.

Meanwhile, the spillover of the conflict is threatening regional stability more and more and that is why the conflict in Mali and the crisis in the Sahel is now a major concern for the entire world, particularly for Europe as we know it.

In short: Why is the Sahel a "Gray Zone"?

- The Sahel is a huge region with high level of conflicts and a low level of development without border controls and rule of law;
- We can find an interaction between big and small powers, between national armies and terrorist groups, involving various types of violence and criminal activities;
- The presence of a terrorist ideology and liberation movements, associated with an extensive traffic of weapons and drugs, and a permanent struggle for power and control over strategic resources made this region a "Gray Zone" and the Mali conflict a "Gray Conflict."

7   Shared Vision, Common Action: A stronger Europe. June 2016 – http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

8   EU-Training Mission in Mali.

9   SPET, Stéphane. "Operation Serval: Analyzing the French Strategy against Jihadists in Mali." ASPJ Africa & Francophonie. 2015/3. – http://www.au.af.mil/au/afri/aspj/apjinternational/aspj_f/digital/pdf/articles/2015_3/spet_e.pdf

10   BLANC, Florent. ECLAIRAGE. De quoi l'Azawad est-il réellement le nom? – Territoires de paix, 14. December 2012 – http://territoires.ecoledelapaix.org/mali/azawad-chabre

THE EUROPEAN UNION'S OPERATIONS IN THE SAHEL

In mid-2011, the EU adopted a comprehensive approach to the Sahel region under the title "Strategy for Security and Development for the Sahel," commonly referred to as the "Sahel Strategy."[11] This Strategy remains the key framework for EU action to help countries in the Sahel region to address key security and development challenges.

- In 2014, EU Foreign Affairs extended the Strategy to Burkina Faso and Chad in addition to Mali, Mauritania and Niger. Ministers also asked for the development of a "Regional Action Plan" for the implementation of the Sahel Strategy.[12] The "Action Plan for the Sahel" was adopted by Ministers of Foreign Affairs on 20 April 2015 and was reviewed and updated in the beginning of June 2016.[13]
- With the establishment of this comprehensive framework for EU's action in the Sahel region, the EU reiterates its readiness to continue working closely with the Sahel countries to support their efforts to achieve peace, security and development. The rule is to support the "Sahel Ownership."

This Strategy has four key subjects:
- First, that security and development in the Sahel cannot be separated, and that helping these countries achieve security is integral to enabling their economies to grow.
- Second, that achieving security and development in the Sahel is only possible through regional cooperation.
- Third, all the states of the region will benefit from considerable capacity building in the area of government activity, including the security and development cooperation.
- Fourth, that the EU therefore has an important role to play in encouraging economic development to achieve a more secure environment in which it can take place, and in which the interests of EU citizens are also protected.

---

11   Strategy for Security and Development in the Sahel. European Union External Action Service. – http://eeas.europa.eu/archives/docs/africa/docs/sahel_strategy_en.pdf

12   Council conclusions on the Sahel Regional Action Plan 2015–2020; 20. April 2015 – www.consilium.europa.eu/en/meetings/fac/2015/04/st07823-en15_pdf/

13   Sahel Regional Action Plan 2015–2020 – http://www.consilium.europa.eu/en/meetings/fac/.../st07823-en15_pdf

Under the Common Security and Defence Policy (CSDP) the EU's comprehensive approach to security and development in the Sahel includes three actions: EUCAP Sahel Niger,[14] EUCAP Sahel Mali and the EU Training Mission in Mali (EUTM Mali).[15]

The restoration of security and peace in Mali is a major issue for the stability of the Sahel region and, in the wider sense, for Africa and Europe.

On 18 February 2013, at the request of the Malian authorities, and in accordance with international decisions on the subject, in particular the United Nations Security Council Resolution 2085 (2012),[16] the European Union launched a training mission for Malian Armed Forces (EUTM Mali). That mission, involving 26 States (22 EU nations[17]) contributing with military personnel (700), is currently under the command of a Belgian Brigadier General.

The aim of the mission is to support the rebuilding of the Malian Armed Forces and to meet their operational needs by providing expertise and advice, in particular as regards operational and organic command, logistic support, human resources, doctrine and education, operational preparation and intelligence, as well as training combat units at the Koulikoro training camp.

The headquarters of the mission is located in Bamako and the training is carried out in Koulikoro (60 km north-east of Bamako). Initially, the mission's third mandate is 24 months. Around 200 instructors have been deployed to Koulikoro training camp, as well as support staff and a protection force, making a total of around 440 personnel and the joint costs of the operation are 28 million Euros for the third mandate of 24 months (18 May 2016 – 18 May 2018).

CONCLUSION AND RECOMMENDATIONS

The Sahel region is a "Gray Zone" and particularly the Mali conflict is a "Gray Conflict" not only for the European Union but also for the entire world. Since global problems can only be solved through global solutions, we need to
- improve the level of interoperability between the Armed Forces of the European Union;

---

14   EUCAP Sahel Niger, – https://eeas.europa.eu/csdp-missions-operations/eucap-sahel-niger_en
15   EU-Training Mission in Mali.
16   United Nations Security Council Resolution 2085/2012 – 20. Dec. 2012.
17   BESENYÖ, J. "Hungarian soldiers in EUTM MALI." IN Tradecraft Review, 2014, 2. Special Issue, pp. 518–125, – http://knbsz.gov.hu/hu/letoltes/szsz/2014_2_spec.pdf

- continue to contribute to the strengthening of the security and defense capacities of the Sahel countries, particularly the Malian Armed Forces as a strong contribution to the stability and development of the Sahel region, and
- adopt an integrated strategy between the European Union and the African Union for the Sahel and engage global partners.

Luís Manuel Brás Bernardino is an Infantry Lieutenant-Colonel at the Portuguese Army, qualified with the Staff Course. He holds a post-graduate diploma in Peace and War Studies in the New International Relations from Universidade Autónoma de Lisboa (UAL), a MA in Strategy from Instituto Superior de Ciências Sociais e Políticas - Universidade Tecnica de Lisboa (ISCSP-UTL) and a PhD in International Relations from the same University. He is a researcher at Centre for Angolan Strategic Studies (CEEA) and is currently conducting academic researches at Centre for International Studies at the University of Lisbon (CEI-IUL) in a project about "African Security and Defence Architectures". He is a member of the International Relations section at the Lisbon Geographic Society, member of the editorial board of Revista Militar and editor of the Revista "PROELIUM" at the Military Academy. Lieutenant-Colonel Luís Bernardino regularly participates in national and international seminars and frequently publishes articles in journals on the subject of security and defence in Africa. He is currently professor of Strategy and International Relations in Department of Post-Graduate Studies (DEPG) at the Military Academy in Lisbon and member of the Centre for Investigation, Development and Research of Military Academy (CINAMIL). He can be reached at: bernardino.lmb@hotmail.com.

BIBLIOGRAPHY

BESENYÖ, J. "*Hungarian soldiers in EUTM MALI.*" IN Tradecraft Review, 2014, 2. Special Issue, pp. 518–125. – http://knbsz.gov.hu/hu/letoltes/szsz/2014_2_spec.pdf

BLANC, Florent. "*ECLAIRAGE. De quoi l'Azawad est-il réellement le nom?*" Territoires de paix, 14. December 2012 – http://territoires. ecoledelapaix.org/mali/azawad-chabre

Council conclusions on the Sahel Regional Action Plan 2015–2020; 20. April 2015 – www.consilium.europa.eu/en/meetings/fac/2015/04/ st07823-en15_pdf/

EUCAP Sahel Niger – https://eeas.europa.eu/csdp-missions-operations/ eucap-sahel-niger_en

EU-Training Mission in Mali – http://www.eutmmali.eu

Mali Central: La fabrique d'une insurrection? International Crisis Group, Rapport Afrique Nº 238 – https://www.crisisgroup.org/fr/africa/west-africa/mali/central-mali-uprising-making

Sahel Regional Action Plan 2015–2020 – http://www.consilium.europa.eu/ en/meetings/fac/.../st07823-en15_pdf

Shared Vision, Common Action: A stronger Europe. June 2016 – http://www. eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

SPET, Stéphane. "*Operation Serval: Analyzing the French Strategy against Jihadists in Mali*" ASPJ Africa & Francophonie. 2015/3. – http://www. au.af.mil/au/afri/aspj/apjinternational/aspj_f/digital/pdf/articles/2015_3/ spet_e.pdf

Strategy for Security and Development in the Sahel. European Union External Action Service. – http://eeas.europa.eu/archives/docs/africa/ docs/sahel_strategy_en.pdf

The Gray Zone, U.S. Special Operations Command, September 9., 2015; p. 1. – https://info.publicintelligence.net/USSOCOM-GrayZones.pdf

United Nations Security Council Resolution 2085/2012 – 20. Dec .2012.

Sources consulted but not cited:

BARNO, David and BENSAHEL, Nora. "*Fighting and Winning in the 'Gray Zone'.*" War on the Rocks, 18. May 2015 – https://warontherocks. com/2015/05/fighting-and-winning-in-the-gray-zone/

BRANDS, Hal. "Paradoxes of the Gray Zone." Foreign Policy Research Institute, 5. Feb. 2016 – http://www.fpri.org/article/2016/02/paradoxes-gray-zone/

Matthew Domingos, Kerin Winarz, Lazar Berman and Yaniv Friedman

On warfare by Proxy

No proceeding is better than that which you have concealed from the enemy until the time you have executed it. To know how to recognize an opportunity in war, and take it, benefits you more than anything else. Niccolo Machiavelli, On the Art of War[1]

Abstract: Throughout history, states have tried to wage warfare "on the cheap," by using others to fight for them.[2] Better to let other states and organizations bleed than one's own soldiers, they reasoned. This idea is at the heart of proxy warfare. While the use of Proxies[3] to achieve foreign policy goals might seem straightforward, the reality is much more complex. Proxy warfare has persisted as technology, political systems, and cultural norms have changed, and as new circumstances develop, proxy warfare itself undergoes fundamental shifts. These changes must be studied in order to develop a model of proxy warfare that is relevant and useful for contemporary realities. This paper examines proxy warfare from the point of view of the Patron. It examines US, Israeli, and Iranian experiences with proxy warfare to identify key similarities and differences in the employment of Proxies in the Middle East. It identifies recurring dangers, roadblocks, and contributors to success and provides a framework for thinking about proxy warfare in order to improve US and Israeli employment of the tool and to inform disruption campaigns against enemy proxy relationships. Synopses of the experiences are provided in the case studies at the conclusion of this report.

---

1   MACHIAVELLI, Niccolo. The Seven Books of the Art of War. The University of Adelaine, 27. March 2016 – https://ebooks.adelaide.edu.au/m/machiavelli/m149a/index.html.
2   MUMFORD, Andrew. Proxy Warfare. Cambridge: Polity Press, 2013; 1.
3   To help alleviate confusion caused by terms with multiple uses, this paper establishes the convention of capitalizing the parties of a Patron-Proxy relationship (e.g. Proxy) and using lowercase when referring to the general subject (e.g., proxy warfare).

EVOLUTION OF PROXY WARFARE

Though proxy warfare has been employed for millennia, the lion's share of the thinking and writing was done during the Cold War period, and largely assumed that two world powers used states and organizations to undermine the other's alliance system. Proxy warfare has changed in significant ways since that time. For a number of reasons, including increased funding sources, the spread of technology, use of the Internet, and the "democratization" of violence,[4] Proxies have more independence from their Patrons than they did during the Cold War.

Today's relationships tend to be less top-down. This phenomenon is especially apparent in the vital issue of funding. As Thucydides observed in his seminal History of the Peloponnesian War, "War is a matter not so much of arms as of money." Today, organizations have more means of funding themselves, thus they are less reliant on their Patron for money.

Patrons often desire deniability, which makes the use of a Proxy the ideal solution to the problem facing them. Deniability has always been a challenge to maintain, but it has become infinitely harder in an age in which smartphones are ubiquitous and images from the battlefield can spread around the globe in a matter of minutes. Communication over the Internet also makes hacking and leaks ever-present dangers to deniability.

During the Cold War, when the strategic environment was relatively stable, Patrons were almost always states, while Proxies took the form of both states and organizations. Without the consistent bipolar strategic backdrop that the Cold War provided, the strategic environment changed rapidly. Ostensibly stable Middle Eastern regimes crumbled in weeks, as sub-state organizations popped up and captured territory before it was clear who they were or what they were after. Today, we see sub-state organizations employing their own Proxies and previously inconceivable alliances, some below the surface, created as new

---

4   HARVEY, Derek. "What is the Democratization of Violence?" 5. October 2014 as quoted in HOFFMAN, Frank. "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War." In 2016 Index of U.S. Military Strength. Washington DC: The Heritage Foundation, 2016. "The term 'democratization of violence' relates to the 'increased and growing access to lethal capabilities contributing to persistent instability and the rising power of non-state actors. The increased access to a range of small arms, crew-served weapons, and indirect fire weapons, and improvised explosive device developments are augmented by the inexpensive, off-the-shelf, innovative technologies being applied by terrorists, rebels, insurgents, protestors and a range of non-state actors such as e.g. small-to-medium size unmanned vehicles/drone, robotics.'"

threats arrive. This dynamic has profound effects on proxy relationships—as the interests of both Patrons and Proxies swing as the strategic environment changes—and should change the way we think about Patrons in general.

LOOKING FORWARD

There is no magic elixir that will guarantee success in war, and while proxy warfare is far from one, it remains an especially relevant tool in a state's kit. While it is fraught with dangers and challenges, proxy warfare can be an extremely advantageous method of damaging one's enemy and promoting one's own interests. The major adversary of the West in the Middle East, the Islamic Republic of Iran, understands the importance of proxy warfare and has employed Proxy organizations to great effect against American and Israeli interests. At the same time, the United States and Israel seem reticent to properly study and employ Proxies in a systematic fashion—a result of past traumas. This imbalance is a major advantage for Iran; without the possibility of carefully planned and managed proxy campaigns, the United States and Israel will continue to face an uphill climb against Iranian interests in the region.

As Western countries consider returning to a broader use of Proxies in the Middle East, their leaders and thinkers will look to the existing body of literature in order to gain a better understanding of the phenomenon. If they do not take into consideration the ways in which proxy warfare has changed, they will be employing a tool in a way that does not match the times. This project is part of the effort to create a relevant body of literature for today's challenges.

The key is to understand when to use Proxies, how to manage the relationship, and how to properly exit the relationship. These are some of the questions this work seeks to address—to provoke critical thought about proxy warfare and ask crucial questions at each stage of proxy warfare execution. This research attempts to identify the recurring challenges Patrons face in their use of Proxies, the inherent risks, and the means of addressing those problems.

Principles of Hybrid Warfare
The fundamental principles of warfare have not changed since man organized into communities that competed for resources. Warfare, as defined here, is a method of political coercion through violent acts. Warfare is not carried out through military power alone. Other tools of the state have always played an important role as well, particularly through diplomatic, informational,

and economic means. The directly attributable use of state military power is typically the means of last resort to achieve a nation's ends.

Within the last several years there has been an increased focus by Western powers on the idea of deliberate management of conflict thresholds, using all of the regional powers' available means to achieve their goals without provoking a major war. This idea has been called several things, from "grey zone," to "hybrid warfare," to "irregular war." However, a nation's use of indirect tools to gain a strategic advantage without provoking all-out war is nothing new for Western nations. As the Finnish scholar Raitasalo notes, "Hybrid warfare is the [reintroduction] of the traditional Great Power logic within shared Western understandings of international security. Hybrid warfare is a Western construction—not a Russian one."[5]

What may be novel is a reinvigoration of the pursuit of strategic objectives through hybrid means, which is free from the fear of reprisals from an international community that seeks to avoid confrontation at all costs. Hybrid warfare represents a return to Machiavellian pragmatism, where the state takes indirect advantage of conflict to achieve political objectives. Proxy warfare is a sub-element of hybrid warfare, and like hybrid warfare, it is still a risky bet—one fraught with the danger of escalation beyond the control of the Patron that initiates it. If the result of proxy warfare action is the initiation of open warfare, then the proxy war failed. If, however, a nation achieves its goals without shedding its own blood, the risk may be worth it.

Principles of Proxy Warfare[6]

Before identifying elements that detract from or contribute to successful proxy warfare, it is important to define the term and identify key principles that shape its use.

Definition of Proxy Warfare

Carelessness in defining the term proxy warfare may result in misleading or vague conclusions, as discussions of the subject often fall victim to vague definitions or sloppy ones that include related, but different, modes of warfare. While proxy warfare is undoubtedly a type of partnership, it is a specific type

---

5   RAITASALO, Jyri. "Some Finnish Findings on RU-UKR War Focusing on Grey Zone and Hybrid Warfare" (Lecture, 2016).

6   The remaining sections of text present original concepts, from the combined JLLD / Dado Center team or JLLD alone, that were developed through extensive research and analysis of historical, open source case studies.

of partnership. Not all alliances are proxy relationships, nor are all outside interventions in local conflict. The authors define proxy warfare as:

A relationship between two entities, be they states or organizations, in which the more powerful actor ("Patron") uses the other to accomplish its foreign policy goals; the less powerful actor ("Proxy") is fighting in a local armed conflict that the Patron wants to influence while limiting its own direct involvement. The two share a common enemy; both envision benefits coming from the relationship; and they coordinate activity during the conflict.

At its most basic, proxy relationships involve a Patron who works through a Proxy to harm the Target. But there are often other players: There can be two or more Co-patrons working directly with the same Proxy. A Patron often works through an Intermediary country or organization to reach the Proxy. A Proxy can even have its own Proxy through which it harms the Target. Oftentimes, more than one of these possibilities are present simultaneously.

Key Principles that Help Define Proxy Warfare
Underlying the concept of proxy warfare are seven key principles that help define its basic characteristics:

Community. The strength of the underlying, unifying strategic goal between the Patron and Proxy is dependent on the strength of community association between the two. Community can involve a shared social, tribal, ethnic, religious, caste, or racial connection that makes the relationship between Patron and Proxy stronger.

Purpose. If multiple Patrons are involved in a proxy warfare campaign against a Target nation, all the Patrons will have a unifying strategic goal. Even if Patrons have secondary goals, there must always be a primary, powerful, and unifying strategic goal.

Aggregation. As the number of Co-patrons increase, the effectiveness of the proxy war in the near term improves, especially if the underlying, unifying strategic goal (described above) is strong and clearly defined.

Time. The Patron's ability to predict the implications of its proxy war decreases over time.

Negative Effect. Proxy warfare is optimal when the desired effect is negative (e.g., to damage a Target nation's assets, degrade government-supported Targets, destabilize a regime). Positive effects such as "nation building" or post-conflict reconstruction by the Proxy should be avoided.

Space. The strength of the relationship between the Patron and Proxy increases when there is a geographic "safe zone" in which the Proxy

can train, plan, work, and recuperate with an Intermediary and/or Patron without fear of attack.

Scope. The likelihood of Patron success improves when the end goal is specific and the proxy warfare campaign scope is limited.

A THEORY FOR SUCCESS: HOW PROXY WARFARE CAN SUCCEED

Proxy warfare is, by its very nature, complex and often requires a long-term commitment that lacks immediate effect. These characteristics may demote proxy warfare as a policy tool, considering the limited strategic patience of most democratic nations. The question is whether proxy warfare remains a viable and effective policy option for most Western nations, and if so, how it might be most effectively implemented to achieve a nation's strategic objectives.

This study does not seek to provide a one-size-fits-all blueprint for Patron-Proxy relationships. However, it does attempt to establish key questions that must be asked and issues that must be examined by the Patron at all stages of proxy warfare. For the purposes of analyzing the core issues and questions, proxy relationships can be divided into three stages: assessing whether to engage in the proxy relationship, managing the proxy relationship, and finally downgrading the proxy relationship.

Assessing Whether to Engage in a Proxy Relationship

One of the steps on the road to war is to determine whether proxy warfare can be a successful tool to leverage. In this light, there are considerations that must first be examined and questions that must be answered.

Considerations for the Use of Proxy Warfare

Proxy warfare can be an effective policy tool when specific conditions are met. These conditions are driven by five considerations that should be examined before any proxy relationship is established:

Absence of Overt Combat by Patron. The Patron *must not be* already engaged in *overt* combat in the conflict area where the intended Proxy is operating. This includes all forms of overt military power. In cases where Proxies—acting as surrogate ground forces—have been supported with *overt* airpower, such as with the coalition operations

in Afghanistan and Libya, success has been limited. Past use of proxy warfare has shown that the when a nation is already invested militarily in a conflict, then that nation's ability to use a Proxy covertly—free from counter-reprisal from the Target—is diminished as well. Instead, a nation should seek out ways in which a conflict can be shaped to benefit a nation's strategic interest without the use of overt force *if the desire is to remain non-attributable*. This may be through political management, economic action, or as is the case with this paper's subject, the use of a Proxy to inflict harm against a Target.

Presence of Overt Combat by Target. The Target *must be* actively engaged in overt combat in the conflict area where the intended Proxy is operating. If the Target is not already engaged in overt action, a Proxy can be used to initiate conflict in order to benefit the Patron.

Extant, Willing Proxy. A viable Proxy must be already extant and willing to enter into a relationship with a Patron.

Strong Proxy Leader. Within the Proxy, there must be an established, strong leader who commands allegiance over viable Proxy forces and who can be influenced by the Patron.

Deniability. The Patron must determine if deniability can be maintained.

QUESTIONS FOR ASSESSING ENGAGEMENT CONDITIONS

Once the potential Patron assesses that the specific conditions are met, the next step is to determine whether or not to enter the proxy relationship—to engage or not to engage. Based on the research for this paper and analysis of the case studies we determined there are several questions to ask. Questions at this stage look to assess whether sufficient shared goals exist in order to initiate a relationship with a Proxy:

What are the Patron's goals?
Can potential Proxies/Intermediaries help the Patron reach those goals?
What will attaining those goals cost the Patron?
Is the Patron willing to pay that price?
Is there a time horizon for the relationship that can be identified at this time?
What could cause the Patron to downgrade the relationship(s)?

CONSIDERATIONS FOR THE USE OF AN INTERMEDIARY

One of the key principles that help define proxy warfare stated that the effectiveness of a Patron-Proxy relationship to achieve identified strategic goals (ends) is greater when based on shared characteristics of community (e.g., ideological, religious, or social mores). A strong relationship between the two parties may lessen the need for employing an Intermediary (although other reasons, such as deniability, may warrant an Intermediary's use). Iran's use of Iraqi Shia militias as Proxies in Iraq and Syria has proved successful in part due to the strong socio-religious identity shared between the Islamic Revolutionary Guard Corps and their Iraqi/Syrian Proxies**.** This is a prime example of Proxy use *without* an Intermediary.

When shared mores between Patron and Proxy do not exist and/or direct engagement is not viable or desired, an Intermediary "surrogate" can be used to achieve the desired ends to increase the likelihood of success (see figure 1). US use of the Pakistani Inter-Services Intelligence (ISI) is an example of the use of an Intermediary with the Mujahedeen in Afghanistan (the Proxy). The Intermediary relationship during the Soviet occupation of Afghanistan helped to pressurize the operational environment for the Soviets and slowly forced their withdrawal. Although this Intermediary relationship did not endure through the ensuing civil war, it is an example of a successful use of an Intermediary to achieve the goal of the Patron.
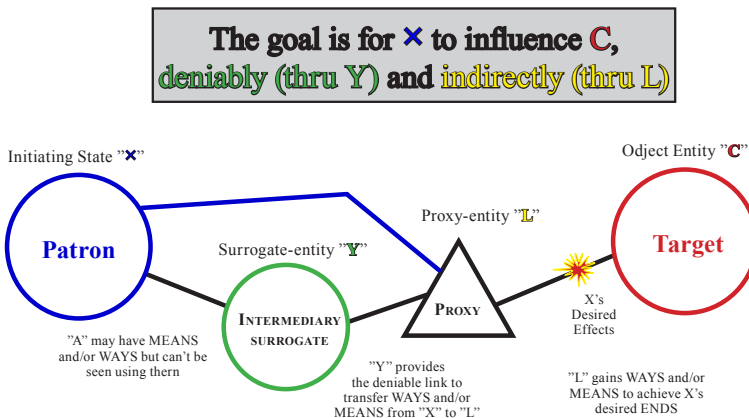
Figure 1.
The Intermediary and the Proxy paradigm

Managing the Proxy Relationship

After the parties have agreed to engage in a proxy relationship, the Patron must manage the alliance. This requires analyzing factors that impact the relationship, assessing the "health" of the relationship, and identifying and overcoming the inevitable tensions that will occur.

Considerations When Engaged in Proxy Warfare

Once the decision to conduct proxy warfare is made, there are other considerations the Patron must analyze to successfully carry out the proxy campaign. These include: clarity of purpose, unity of effort, precision of focus, maintaining the advantage, and strategic patience.

Clarity of Purpose. Define strategic objectives and policy direction so they are unambiguous (simple, direct, and clear) and assess and accept the risk of short- and long-term implications.

Unity of Effort. Reinforce Proxy and Intermediary (if applicable) restraint to prevent open conflict with the Target. Secondary or hidden goals must be passively or actively accepted when other Co-patrons become involved. The secondary goals of the Co-Patron, if they exist, must also be accepted by the Primary Patron.

Precision of Focus. Avoid the devolution of proxy warfare into stability operations and/or nation building to reduce Patron exposure and prevent expansion of operations beyond the original intent (i.e., "mission creep").

Maintaining the Advantage. Provide tailored aid that is lethal and adaptable but maintains a measure of deniability and reduces the Target's operational advantage.

Strategic Patience. Recognize that covert force and deniability require strategic patience. The Patron should balance deniability and the achievement of goals, while avoiding undesired escalation.

ASSESSING A PROXY RELATIONSHIP

Also based on the research for this paper and analysis of the case studies, we determined the next set of considerations that seek to assess where the relationship stands at a given time and what trends exist:

Determine whether the advisors are maintaining Patron control over the Proxy or whether they are they "falling in love" with the local partners with whom they are working.

The Patron should assess the potential benefits of using multiple Proxies.

One body should manage the relationship, in order to avoid a turf war.

A red team should be established to continuously assess the relationship from the outside, in order to recognize strategic change.

The Patron should develop strategic and operational metrics in order to continuously assess the relationship (also monitored by the red team).

The control that the Intermediary (if there is one) enjoys over the relationship should be recognized and taken into consideration.

Inherent Tensions in Patron-Proxy Relationships

Regardless of the specific actors and context, there exist inherent tensions in Patron-Proxy relations. These tensions are manageable if recognized, but do place stress on the relationship:

Differing Goals. Though there must be some overlap in order to work together, Patron and Proxy goals are never completely identical. Each side has its own interests, and to some extent uses the other to attain what it wants. Moreover, the goals of both sides evolve as the conflict progresses, changing the stresses on the relationship.

Ethics and Norms. Another tension between the Patron and Proxy is that of ethics and norms. Western powers like the United States and Israel have (and attempt to adhere to) strict legal and ethical codes of conduct in war; local Proxies often do not. Their use of violence can cause embarrassment or worse for Western Patrons.

Governed by Self-interest. Tensions between the actors go beyond those of the Patron and Proxy. There are often two or more Patrons working with a Proxy, each with its own fluid interests. In addition, in cases where a Patron works through an Intermediary, both parties will operate according to their own needs and desires, which will inevitably create tension at some point in the relationship.

Cost-benefit Equation. There are a number of tensions that are specifically applicable to the Patron. It must deal with the trade-off between pursuing actions that could bring benefit in the short term, but also come with long-term costs. This cost-benefit equation is important to keep in mind especially concerning pressures by Proxies to pull Patrons more deeply into conflicts.

Influence and Control. Another tension related to costs of involvement revolves around the issue of influence and control. A Patron naturally wants to wield maximum influence over its Proxy, as it is using the Proxy to achieve its own foreign policy goals. Greater influence usually means greater investment and involvement. But this means the Patron is paying a higher price—in resources, political fallout, and even human life—than it would if it settled for reduced control. The benefits of the alternative paths shift during a conflict, and the Patron must reassess accordingly.

Overt and Covert Operations. Tensions exist regardless of whether support is overt or covert. There are benefits to a Patron operating overtly: it increases credibility and allows the Patron to take credit for successful campaigns. On the other hand, covert support for Proxies allows the Patron to avoid costs associated with involvement in a conflict. This tension must be resolved by Patrons before entering a conflict, and will likely need to be reconsidered as the conflict progresses.

Deciding Whether to Downgrade. The final tension revolves around the decision whether or not to downgrade the relationship. Maintaining the relationship with the Proxy enhances the Patron's credibility, in the eyes of the Patron and in the eyes of the world if the relationship is overt. But self-interest usually dictates that at some point, the Patron should downgrade or end its relationship with the Proxy. There is often a significant cost associated with maintaining or deepening the relationship, as there is with withdrawing from the relationship.

In order to properly address the tensions, the Patron must be fully aware of tensions that exist (or are likely) as it decides to initiate and subsequently maintain the proxy relationship. The Patron—whether it is the United States or Israel—will have to make its own determination on how it wishes to address each of these tensions, based on the specific circumstances with which it is dealing.

Controlling the Proxy

While in a relationship with a Proxy, the Patron possesses several tools for managing the Proxy. Ultimately, the Patron wants to be able to control the Proxy to the greatest extent possible, but as noted, friction and disagreement(s) will occur. If the Patron finds itself unable to sufficiently influence or control its Proxy, it has a number of means of applying pressure to coerce it back into line:

The Patron can change the level of aid (e.g., military, medical, financial) it is providing.

The Patron can reduce its diplomatic support for the Proxy.

The Patron can transfer resources to a rival Proxy, sending the message to the recalcitrant Proxy that it is not indispensable.

The Patron can improve relations with the Target nation/organization at the expense of the Proxy.

DOWNGRADING THE PROXY RELATIONSHIP

Patron-Proxy relationships are similar to attacks, in that at some point, friction becomes so great that continued efforts on the part of the Patron have diminishing returns and open it to counterattacks, rather than bringing additional gains. This is called the *culminating point*. It is crucial that the Patron achieve its goals and disengage before the culminating point is reached.

It is, however, inevitable that at some point the Patron will look to disengage (at least to some degree). If the goals shared by the Patron and Proxy no longer sufficiently overlap or diverge completely, it is time to examine downgrading the relationship. The following considerations will help manage this complex process—one that bears risk and requires manifest deliberation and care.

Priority should be given to the red team's assessment on disengagement over recommendations by the body managing the relationship.

It is preferable to disengage *before* a crisis between Patron and Proxy occurs, and not during the crisis.

The Patron should take the long view, weighing the possibility of a gradual downgrade or rebalance instead of a clean break, as it may well need to restore the relationship in the future.

The Patron should also consider how to disengage without leaving a vacuum behind that could wipe out gains and even pull the Patron back into the conflict.

Conclusion: Is Proxy Warfare a Viable Policy Option for a Modern Democratic Nation?

The proxy warfare case studies analyzed in this project illustrate the shared motivations and variables vital to Patrons' assessments of whether to use a Proxy. Mutual motivations that can form a link between a Patron and a Proxy include: local interests, religion and ethnicity concerns, and ideology-based geopolitical views. Further, our research highlights key variables within the Patron-Proxy relationship for the Patron's consideration: the potential for

changes within the operational environment, evolution of goals over time, planning for—and anticipating— strategic change, geographic proximity to the Target, and using an Intermediary with their Proxy. Additionally, the influence of a strong Proxy leader can also work in the Patron's favor as a means to aid local legitimacy and translate goals into action. This project isolated three main phases of proxy warfare; though these phases have not been utilized consistently by Patrons in the past, they do present a recipe for future potential success:

Assessing Engagement Conditions. The decision by a Patron on whether to engage in proxy warfare depends on whether the shared goals with the Proxy are sufficient to initiate a relationship. If the Patron opts to engage in proxy warfare, management of the ongoing relationship is vital; in particular, the Patron must consider the potential costs in using a Proxy group, potential time limitations, and factors that could ultimately cause the Patron to downgrade the relationship.

Managing the Relationship. As the Proxy's goals can diverge from those of the Patron over time, the Patron can take multiple steps, including tightening its control over the Proxy and refining strategic and operational metrics, to continuously assess the relationship. To manage the Proxy, Patrons can vary the type and amount of aid provided and transfer resources to rival Proxy groups. Patrons also could improve relations with the Target, at the expense of the Proxy, or change the level of diplomatic support it is providing. Additionally the Patron can shift its level of control over an Intermediary within the Patron-Proxy relationship.

Disengaging from Proxy Warfare. Patrons must consider the consequences of disengaging amid a crisis or before one potentially occurs. Patrons could take a longer view and consider gradually downgrading the relationship over time. While it is beneficial for a Patron to attempt to disengage without creating a vacuum, there are limitations. For example, some Patron nations may have such a close geographic proximity to a conflict that continued engagement with a Proxy may be necessary. In these specific cases disengagement from a Proxy may have existential ramifications.

Case Studies

What follows are case studies based on US, Israeli, and Iranian experience with proxy warfare. Their purpose is to provide real-world examples of

common characteristics found in the employment of Proxies in the Middle East.

As these case studies illustrate, the experiences of Patrons engaged in proxy warfare are dependent on multiple factors. The US experience in Afghanistan and Israel's use of the Maronite Christians highlight the impact of timing a Patron's withdrawal from proxy warfare and the consequences of the Patron's exit over the long term. The nuances within the Patron-Proxy relationship are also significant: the US-backed New Syrian Forces (NSF) was targeted because of its affiliation with the United States, yet the religious ties between Iran and Hezbollah enabled an enduring link between Patron and Proxy and contributed to Iran's pursuit of its regional goals.

United States and Mujahedeen

The United States' use of the Mujahedeen against the Soviets and their surrogate government, the People's Democratic Party of Afghanistan, during the Soviet occupation is well known. From 1979 until the Soviet withdrawal in 1989, total aid to the Mujahedeen via the Pakistani ISI reached over 2 billion dollars.[7] Saudi Arabia, one among many Co-patrons, matched every cent along the way. In December of 1979, the initial investment made by the Carter administration was small ($ 500,000) and limited (non-lethal aid and small arms).[8] The program expanded during the Reagan administration, culminating with the National Security Decision Directive 166 (NSDD 166) (1985) that pushed Operation Cyclone to the edge of plausible deniability. The aggressive push after this directive was released facilitated the introduction of US-made Stinger missiles into the conflict. Even with the introduction of a US-made and capable weapon, the veil of deniability was maintained throughout the proxy warfare campaign. The United States successfully provided lethal and effective aid to its Proxy without crossing thresholds and pushing the Soviet Union into the frightening proposition of an all-out war between two nuclear-armed nations.

During this operation, the United States stayed out of the fight by using the ISI as an Intermediary; this also mitigated international perceptions of direct American meddling. This obfuscation maintained the political and military leverage the United States needed for a long, indirect proxy fight

---

7   RAITASALO. "Some Finnish Findings on RU-UKR War Focusing on Grey Zone and Hybrid Warfare."
8   HUGHES, Geraint. My Enemy's Enemy. Eastbourne: Sussex Academy Press, 2014.

against the Soviets. By using its Proxy the United States avoided a direct confrontation with the USSR while achieving its goal of inflicting pain—free from reprisal—and creating pressure that influenced a Soviet withdrawal.

The main US strategic goal, also outlined in NSDD 166, was to expel the Soviets from Afghanistan.[9] This was a specific and clearly communicated strategic goal around which the United States and its elements of power could rally. The goal was at least passively accepted by the Co-patrons (Saudi Arabia and Egypt among others) as evident by their continued participation and support.[10] Other minor motivational factors did not detract from the primary and unifying objective.

However, despite the initial success of the Soviet withdrawal, there were long-term implications which devolved into long-term problems. The Soviet withdrawal precipitated a political void that provided a sanctuary for the rise of the Taliban during the ensuing civil war. Such long-term implications cannot always be predicted. Whether overtly or implicitly, the United States deemed the risk of future consequences to be less important than the near-term US Cold War strategic aims against the USSR. The United States recognized the advantage and correctly focused its effort to increase leverage, while accepting the possibility of future risks and unknowable consequences. In other words, the United States chose the lesser of the two evils.

Dado Center: Israel and the Maronite Christians
Even before it gained independence, Israel sought to build alliances with other minorities in the Middle East to mitigate its isolation in the region with its Arab-Muslim majority. The Jewish state succeeded in creating deep ties with the Kurds, Iran, and Turkey among others. The Maronite Christian community in southern Lebanon also fit naturally into this framework.[11]

TENTATIVE AID
Relations with the Maronite community, especially villages in southern Lebanon, predate Israel's independence. Israel initially sought intelligence on hostile actors in Lebanon, while the Christians wanted arms for their fight

---

9   U.S. Policy, Programs and Strategy in Afghanistan. National Security Decision Directive Number 166, 27. March 1985. Declassified on 22. April 2010.
10   MUMFORD. Proxy Warfare.
11   EVRON, Yair. War and Intervention in Lebanon–The Israeli-Syrian Deterrence Dialogue. Baltimore: Johns Hopkins University Press, 1987; 28.

against rival groups in the country. But the relationship deepened, and both sides brought increasing expectations to the table as the decades passed.[12]

In 1958, the Lebanese Christian-dominated government of Camille Chamoun faced an existential threat. Muslim forces supported by Nasser's Egypt and by Syria sought to topple the government and replace it with a Nasserite regime. As a result, Chamoun requested support from Israel.[13]

Israel tried to balance between supporting Chamoun and not being dragged into a conflict to which it was not a party. Israel began supplying weapons to Christian villages in south, and in return, Israel received intelligence. Israel also sent aid to the Christians in the north through Iran, (also an enemy of Nasser); the Iranian channel allowed Israel to maintain deniability.[14]

Israel offered some diplomatic assistance as well. The Maronites asked Israel to petition the United States for more aid, which Israel agreed to do, but they received a cold response from Washington.[15]

In 1975, a bloody civil war broke out in southern Lebanon, which led to a Syrian incursion in 1976. Israel and Syria came to secret mutual understandings about force deployment In Lebanon, known as the "red-line understandings." Israeli leaders debated how to deal with this new reality. Prime Minister Yitzhak Rabin opposed military involvement in the civil war, while his foreign and defense ministers wanted to seize the opportunity to strengthen the alliance with the Christians.[16]

The collapse of the Lebanese Army's 1st Brigade in March 1976, as a result of the civil war, left Christian villages in the south vulnerable to the Palestine Liberation Organization (PLO).[17] Israel wanted to ensure that PLO forces did not move into the border region. The shared anti-PLO interest led to closer ties between the Maronites and Israel. Israel supported local defensive enclaves in southern Lebanon, providing Christians with communications gear, military advice, and even artillery support against the PLO. The close ties spread to more Christian villages, and Israel began allowing Lebanese Christians into the country for medical services and businesses. Still, Israel managed to maintain its policy of restraint, and kept ground troops and its air force out of

---

12   EITAN, Raphael (also Raful Eitan). A Soldier's Story: The Life and Times of an Israeli War Hero. Tel Aviv: Maariv, 1985; 153.
13   Ibid.
14   Ibid.
15   Ibid.
16   MAISEL, Erez. "Transition Period: The Aid Initiative to the Residents of South Lebanon." The Dado Center Journal. 1, Tel Aviv: The Dado Center, 2014. 124–120, Hebrew edition.
17   MAISEL. "Transition Period," 124–120.

the fight. However in November 1976, Israel gave up its attempts to keep its support quiet when it launched a major artillery strike to support Maronites forces; this marked the shift to overt support.[18]

Escalation into Overt Action

A new Israeli government under the Likud Party's Menachem Begin came to power in 1977, and with it, Israeli operations against the PLO continued to intensify. As the PLO's power grew, Maronites increasingly called on Israel to increase its aid.[19] But it took the March 1978 PLO bus hijacking that left 38 Israelis dead for Israel to move ground forces into Lebanon.[20]

Operation Litani, Israel's response to the attack, was designed to strike at the PLO, but not to create a new political order in Lebanon. Another goal was to create a security zone up to the Litani River, patrolled by the Christian militia of Major Said Hadad. The operation resulted in the United Nations Interim Force in Lebanon, created to separate the warring parties.[21]

Operation Litani was Israel's departure from its previous policy of restraint in Lebanon. Still, the escalation was not a result of an Israeli desire to protect the Maronites (though they had caused a steady escalation up to that point), but was the result of PLO attacks.[22]

With the second Begin administration in 1981, Israeli embarked on a new policy in Lebanon. The policy of restraint was officially ended. The focus of Israel's outreach was the Christians in the north. From the goal of helping the Maronites help themselves, Israel now sought to create a new regional order; it wanted: the PLO and Syrian forces entirely out of Lebanon, Christians in charge of the government, and a bilateral peace agreement.[23]

In the meantime, Syria shifted from supporting the Christians to supporting the PLO. The danger of Syria capturing the Christian villages changed the situation for Israel. When Christian leaders in Beirut begged Israel to combat Syrian airpower, Israel agreed—shooting down two Syrian helicopters involved in operations against Christians. This was a major turning point,

---

18   EVRON. War and Intervention. 45.
19   EVRON. War and Intervention. 71–73.
20   RABINOVICH, Itamar. The War for Lebanon 1970-1983. Ithaca and London: Cornell, 1984; 107.
21   Ibid.
22   Ibid.
23   SCHIFF, Ze'ev and YA'ARI, Ehud. Israel's Lebanon War. Jerusalem and Tel Aviv: Shocken, 1984; 38–32, Hebrew edition.

as Israel engaged Syrian forces, not as a response to Syrian actions against Israel, but in support of Christians.[24]

A string of PLO attacks abroad was the proximate cause for the First Lebanon War in 1982. The conflict saw Israel drive as far north as Beirut, expel the PLO, and install a Christian-led government that signed a (short-lived) peace agreement with Israel.[25]

Israel's strategy and very purpose in supporting Lebanese Christians changed drastically from the pre-state period until the invasion of Lebanon. From quietly helping Christians in the south to help themselves, the effort expanded to supporting Christians in the north—an attempt to change the political order in the country through a major military operation. Of course, it was in the Maronites' interest all along to have Israel as deeply involved in Lebanon in possible.

The goals of both sides expanded over the years, as the situation developed and ties grew stronger. The expansion of support depended on the rise of political leaders who were determined to advance the relationship—Begin and Sharon on the Israeli side, and Gemayel on the Maronite's. The fact they shared a clear common enemy in the PLO, and later the Syrians, was an important factor contributing to the stability of the relationship. The historical connection and familiarity between the sides helped keep the relationship smooth during times of stress. Though the sides were not part of the same religious community, they were in similar circumstances as non-Muslim minorities in the Middle East. The geographic proximity also served as a stabilizing factors, making the transfer of people, intelligence, and aid much easier.

Reflections from the Israeli Perspective

The "Lebanon trauma"—Israel's experience in Lebanon, from its tentative aid to Maronites through the full-blown occupation of southern Lebanon—left a deep scar on the Israeli consciousness that colors all debate around Israel's approach to proxy warfare. There emerges a distinct Israeli model of proxy warfare The Israeli attempt at regime change in Lebanon (as part of creating a new regional order) is the dominant proxy experience in Israeli minds. It is the reason that all the Israeli cases are historical, as Jerusalem stayed away from proxy warfare after its struggles in Lebanon. Recognizing the prominence

---

24   RABINOVICH. The War for Lebanon 1970–1983; 116–117.
25   Ibid.

of the Lebanon case will help Israel more openly and objectively study the possibility of proxy warfare as a relevant tool for contemporary challenges.

Even with the dominance of the Lebanon experience, patterns arise throughout the Israeli involvement in proxy warfare since 1948:

Israel has shown a preference toward covert proxy relationships, for understandable reasons. Most of its Proxies, especially vulnerable Muslims like the Kurds, would suffer even more if the fact of their cooperation with Israel was widespread knowledge. Though Israel would gain in terms of credibility were its relationships overt, the complex dealings with Proxies were far simpler when they remained quiet. The major exception to this is the Israel–South Lebanese Army relationship, which ended poorly in Israeli eyes.

While the United States and other major powers use Proxies around the world, Israel focused its efforts on the Middle East and its periphery. Though it has military relationships in distant regions, it lacks both the resources and the interests in developing proxy relationships beyond the Middle East. The idea of close proxy relationships on the periphery of hostile Arab-Muslim states guided Israeli policy for decades, and to some extent still does.

When it does use Proxies, the aid is primarily military, with some sporadic civil aid. There is one case in which Israel tried to leverage a range of military and civil capabilities to aid its Proxies and southern Lebanon. This was made possible both by political will and geographic proximity. Civilians and fighters from its Lebanese proxy could easily cross the border into Israel for business and medical care, and the relationship had a momentum that pushed it toward expansion.

Throughout its experience, there are recurring patterns in Israel's use of regional Proxies that have limited its success:

There is not one dominant body responsible for employing Proxies, as there is in Iran. Instead, each case is different, with the Israel Defense Forces, Mossad, Prime Minister's Office, and Foreign Ministry taking different roles in each case. At times the various government agencies would work together, and at times would find themselves working at cross-purposes.

In addition, and likely as a result of the above pattern, Israel consistently struggled to develop exit conditions and make sense of strategic changes. There was not an organized effort to stand back and observe the relationship, and continuously understand what strategic changes had occurred and whether the proxy relationship was still relevant and beneficial for Israel.

Instead, Israel found itself being dragged deeper into situations against its strategic interests.

United States and the New Syrian Forces

During the Syrian Civil War, the United States used proxy warfare to counter the Islamic State of Iraq and Syria (ISIS) in Syria. As a Patron, the United States proxy warfare efforts against its Target, ISIS, were hindered by an al-Qaeda-linked Adversary (Jabhat al-Nusra [JN]) and the disproportionately small size of its Proxy element in the target area. Further complicating the US use of the New Syrian Forces (NSF) was the Proxy's competing goals and overt affiliation with its Patron.

Recruited from the opposition Free Syrian Army, the NSF were tasked with a counter-ISIS mission:[26]

The United States will train and equip appropriately vetted elements of the Syrian armed opposition. The program, through the Department of Defense, will help moderate Syrian fighters . . . stabilize areas under opposition control and empower a subset of the trainees to go the offensive against [ISIS].[27]

US support of the NSF centered on training and equipping the Proxy group in Turkey, then embedding it within another unit (Division 30).[28] Use of Division 30 was intended to enhance the NSF's ability to target ISIS, as they would be led by individuals familiar with the territory and operational environment.[29] The United States vetted potential members, to weed out radical Islamists and ensure their commitment to the counter-ISIS mission.

The NSF was too small and had limited capability to challenge ISIS. As the United States drew its Proxy members from Syrians who were anti-regime, stringent vetting significantly reduced the number of potential members. Additionally, individuals who were recruited for the NSF did not graduate from US-provided training, and many of the soldiers who left the Syrian military to join the opposition were not the forces' strongest, most

---

26   WELNA, David. "Syrian Rebels Will Face ISIS, but the US May Not Have Their Backs," National Public Radio, 14. March 2015 – http://www.npr.org/2015/03/14/392945308/syrian-rebels-will-face-isis-but-the-u-s-may-not-have-their-backs.

27   "Syrian Crisis: US Assistance and Support for the Transition." US State Department, Fact Sheet, 29. September 2014 – https://www.state.gov/r/pa/prs/ps/2014/09/232266.htm

28   "Syrian Crisis." US State Department; WHITE, Jeffrey. "The New Syrian Force: Down but not Necessarily Out." The Washington Institute, 11. August 2015 – http://washingtoninstitute.org/policy-analysis/view/the-new-syrian-force-down-but-not-necessarily-out.

29   WHITE. "The New Syrian Force."

capable fighters. As a result, the NSF was a much smaller force than intended (numbering approximately 60).[30]

The NSF's affiliation with the United States in this overt Patron-Proxy relationship rendered it a target of anti-US sentiment in Syria. This was highlighted when the NSF was attacked by JN.[31] The United States had previously carried out airstrikes on JN-associated groups, dating back to September 2014.[32] US airstrikes on 8 July 2015 were reported to have killed a key JN-affiliated leader.[33] As a result, the group developed animosity towards the United States and individuals it believed to be collaborating with the United States.[34] NSF claimed their 30 July 2015 attack was in retribution to prior US attacks.[35]

While this US train-and-equip program ended in October 2015, this instance of proxy warfare had several advantageous attributes:[36]

A shared goal of defeating ISIS.

An employment concept of embedding the Proxy into an Intermediary group, which provided the NSF greater awareness of the environment.

Dedicated Patron support, as US airstrikes provided essential backup for the Proxy following the JN attack.[37]

Supportive external regional partners (Turkey and Jordan) provided safe training areas for the Proxy members.

Other factors in this Patron-Proxy relationship remained persistent challenges:

Anti-US adversaries attrited the Proxy in the short term, thus defeating the Patron's longer term aims.

Competing goals comprised effective US vetting, as many Proxy members retained high interest in their original goal of toppling the Assad regime.

The Proxy was hindered by its small size and limited skills.

---

30   Ibid.
31   Mapping Militant Organizations Project. Stanford University, 1. October 2015 – http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/493.
32   WELNA. "Syrian Rebels"; WHITE. "The New Syrian Force."
33   Mapping Militant Organizations Project.
34   Mapping Militant Organizations Project; WHITE, "The New Syrian Force."
35   WHITE. "The New Syrian Force."
36   SHEAR, Michael COOPER, Helene and SCHMITT, Eric. "Obama Administration Ends Effort to Train Syrians to Combat ISIS," New York Times, 9. October 2015 – http://www.nytimes.com/2015/10/10/world/middleast/pentagon-program-islamic-state-syria.html.
37   WHITE. "The New Syrian Force."

IRAN AND HEZBOLLAH

Iran, acting as a Patron, experienced some success in executing proxy warfare against a Target group (anti-regime rebels in Syria) as a result of having a shared religious background with its Proxies, maintaining clear strategic aims, and through frequent use of a capable Intermediary/Partner (Hezbollah) when necessary.[38] At times, the Proxy's successes were curbed by the Patron's focus on other regional activities.[39]

During Syria's Civil War, Iran used proxy warfare to support the regime.[40] Using both Hezbollah and Iraqi Shia militias, Iran worked to support Assad against attacks by opposition forces and regain control over his country.[41] While Iran was limited by its own competing strategic goals and changing dynamics (e.g., ISIS gains in Iraq) that required it to shift levels of support to its Proxies in the region, it was successful in its use of proxy warfare in Syria because:[42]

Shared religious affiliation: Iran and its Proxy are linked by their shared belief in Shia Islam, which enables strong links and commonalities.[43]

Enduring strategic goals and assured continuity of Patron's leadership.

Capable Intermediary: Hezbollah filled multiple roles for Iran that were supportive of Iran's goals (i.e., Proxy, Intermediary, Partner/Co-Patron).[44]

Flexibility: The Patron deployed its own military advisors when necessary into the operational area.[45]

Experience: The Patron had decades of experience using proxy warfare throughout the region, particularly with Shia militias.[46]

---

38   KNIGHTS, Michael. "Iran's Foreign Legion: The Role of Iraqi Shiite Militias in Syria," The Washington Institute, PolicyWatch 2096; 27. June 2013 – http://washingtoninstitute.org; BERTI, Benedetta. "Proxies, Partners-State and Non-States," Presentation at the IDF Dado Center, 16. August 2016.

39   MCINNIS, Matthew. "Iran's Strategic Thinking: Origins and Evolution," American Enterprise Institute, May 2015; ii, 4, 15–17, 20 – https://www.aei.org/wp-content/uploads/2015/05/Irans-strategic-thinking.html.

40   SMYTH, Phillip. "How Iran is Building its Syrian Hezbollah," The Washington Institute, PolicyWatch 2580; 8. March 2016 – http://washgintoninstitute.org.

41   BERTI. "Proxies, Partners-State and Non-States."

42   DAOUD, David. "Meet the Proxies: How Iran Spreads its Empire through Terrorist Militias," accessed 10. August 2016 – http://www.thetower.org/article/meet-the-proxies-how-iran-spreads-its-empire-through-terrorist-militias; MCINNIS. "Iran's Strategic Thinking."

43   BERTI. "Proxies, Partners-State and Non-States."

44   DAOUD. "Meet the Proxies."

45   KNIGHTS. "Iran's Foreign Legion."

46   MCINNIS. "Iran's Strategic Thinking"; DAVID DAOUD, "Meet the Proxies."

Matthew Domingos is Lieutenant Commander in the US Navy. Between 2002 and 2015 he served in a variety of naval operational and staff billets as well as positions in support of Operations IRAQI FREEDOM and ENDURING FREEDOM. He was awarded the Bronze Star, the Joint Commendation Medal, the Navy Commendation Medal (two awards) and the Air Force Commendation Medal. LCDR Domingos Since 2015 he has worked as an analyst supporting the Joint Staff J7's Joint Lessons Learned Division's Joint and Coalition Operational Analysis branch.

Kerin Winiarz has directly and indirectly supported the Department of Defense since 2007. She has worked as an analyst for Science Applications International Corporation (SAIC) since 2015, supporting the Joint Staff J7's Joint Lessons Learned Division's Joint and Coalition Operational Analysis branch. In 2007, Ms. Winiarz worked for the Defense Intelligence Agency (DIA), focusing on political-military issues and foreign influence. Additionally, Ms. Winiarz has been awarded two Office of the Director of National Intelligence (ODNI) awards; in 2013, she received the ODNI's National Intelligence Professional Award in recognition of her contributions to a major cross-agency project.

Lazar Berman holds an MA in Security Studies from Georgetown University. His thesis examined Israeli military innovation from 2000-2009. He was an editor at The Times of Israel, and taught at Salahuddin University in Erbil, Iraq. He previously served as an infantry officer in the IDF.

Yaniv Friedman holds an MA in International Relations and History from Haifa University. His thesis examined Israel's security concept under Golda Meir. Friedman worked as a researcher in the National Security Studies Center at Haifa University, and is currently writing his doctoral dissertation at Tel Aviv University on the Eshkol Administration's security policies. He previously served as a reconnaissance squad commander in the IDF.

BIBLIOGRAPHY

BERTI, Benedetta. "*Proxies, Partners-State and Non-States*" Presentation at the IDF Dado Center, 16. August 2016.

DAOUD, David. "*Meet the Proxies: How Iran Spreads its Empire through Terrorist Militias*" accessed 10. August 2016 – http://www.thetower.org/article/meet-the-proxies-how-iran-spreads-its-empire-through-terrorist-militias;

EITAN, Raphael (also Raful Eitan). *A Soldier's Story: The Life and Times of an Israeli War Hero.* Tel Aviv: Maariv, 1985; 153.

EVRON, Yair. *War and Intervention in Lebanon–The Israeli-Syrian Deterrence Dialogue.* Baltimore: Johns Hopkins University Press, 1987; 28.

HARVEY, Derek. "*What is the Democratization of Violence?*" 5. October 2014; quoted in HOFFMAN. "*The Contemporary Spectrum of Conflict*"

HOFFMAN, Frank. "*The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War*" In *2016* Index of U.S. Military Strength. Washington DC: The Heritage Foundation, 2016. HUGHES, Geraint. *My Enemy's Enemy.* Eastbourne: Sussex Academy Press, 2014.

KNIGHTS, Michael. "*Iran's Foreign Legion: The Role of Iraqi Shiite Militias in Syria*" The Washington Institute, PolicyWatch 2096; 27. June 2013 – http://washingtoninstitute.org;

MACHIAVELLI, Niccolo. *The Seven Books of the Art of War.* The University of Adelaine, 27. March 2016 – https://ebooks.adelaide.edu.au/m/machiavelli/m149a/index.html.

MAISEL, Erez. "*Transition Period: The Aid Initiative to the Residents of South Lebanon*" The Dado Center Journal. 1, Tel Aviv: The Dado Center, 2014; 124–120, Hebrew edition.

Mapping Militant Organizations Project. Stanford University, 1 October 2015 – http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/493.

MCINNIS, Matthew. "*Iran's Strategic Thinking: Origins and Evolution*" American Enterprise Institute, May 2015; ii, 4, 15–17, 20 – https://www.aei.org/wp-content/uploads/2015/05/Irans-strategic-thinking.html.

MUMFORD, Andrew. *Proxy Warfare.* Cambridge: Polity Press, 2013; 1.

RABINOVICH, Itamar. *The War for Lebanon 1970–1983.* Ithaca and London: Cornell, 1984; 107.

RAITASALO, Jyri: "*Some Finnish Findings on RU-UKR War Focusing on Grey Zone and Hybrid Warfare*" (Lecture, 2016).

SCHIFF, Ze'ev and YA'ARI, Ehud. *Israel's Lebanon War.* Jerusalem and Tel Aviv: Shocken, 1984; 38–32, Hebrew edition.

SHEAR, Michael – COOPER, Helene and SCHMITT, Eric. "*Obama Administration Ends Effort to Train Syrians to Combat ISIS*" New York Times, 9. October 2015 – http://www.nytimes.com/2015/10/10/world/middleast/pentagon-program-islamic-state-syria.html.

SMYTH, Phillip. "*How Iran is Building its Syrian Hezbollah*" The Washington Institute, PolicyWatch 2580; 8. March 2016 – http://washgintoninstitute.org.

"*Syrian Crisis: US Assistance and Support for the Transition*" US State Department, Fact Sheet, 29. September 2014 – https://www.state.gov/r/pa/prs/ps/2014/09/232266.htm

U.S. Policy, Programs and Strategy in Afghanistan. National Security Decision Directive Number 166; 27. March 1985. Declassified on 22. April 2010.

WELNA, David. "*Syrian Rebels Will Face ISIS, but the US May Not Have Their Backs*" National Public Radio, 14. March 2015 – http://www.npr.org/2015/03/14/392945308/syrian-rebels-will-face-isis-but-the-u-s-may-not-have-their-backs.

WHITE, Jeffrey. "*The New Syrian Force: Down but not Necessarily Out*" The Washington Institute, 11. August 2015 – http://washingtoninstitute.org/policy-analysis/view/the-new-syrian-force-down-but-not-necessarily-out.

Robert J. Elder and Alexander H. Levis
A Gray Zone Challenge: Intent and Military Response

Abstract: Mapping political, security, societal and economic trends to the decision calculus of key regional and (as applicable) non-state actors has been used to gain insights into the behaviors of actors conducting multi-instrument operations in the "gray zone" between peace and conflict. Timed Influence Net (TIN) models have been used to identify potential sources of strategic risk, and serve as the foundation for a planning framework designed for use by operational planning teams to support operational and engagement planning by Combatant Commands and their components. Computational experiments were performed using the TIN models. The computational experiments focused on gray zone actor perceptions of the decision calculus to counter the effects of gray zone activities.

Introduction

This paper discusses the use of escalation control principles and deterrence theory to reduce risk from gray zone activities. The "Gray Zone" has been notionally defined as an adversary's purposeful use of single or multiple elements of power to achieve security objectives by way of activities that are ambiguous, cloud attribution and exceed the threshold of ordinary peacetime competition yet fall below the level of militarized threats to a state's security interests. These activities threaten targeted entities (states, alliances) by challenging, undermining, or violating international customs, norms, or laws. An alternative definition is that the gray zone is the purposeful application of multiple elements of power—information, economic, military, political—to achieve objectives in ways that exceed the threshold for normal competition yet fall below the level of major interstate war. The purpose of gray zone conflict is to avoid major power war and costly penalties, hinder an effective

response by intentionally blurring peacetime and wartime operations, and control escalation.

We have adapted a commonly used deterrence definition to examine the decision calculus of Actor 'X" regarding Action 'Y' under Condition 'Z' leveraging earlier work.[1] The actors of interest in this definition have been identified, and the condition of interest can be generally described as an environment characterized by the conduct of gray zone activities. It is a commonly accepted assumption that the home country and its partners (the targets of the gray zone actor) would want to deter gray zone activities. In this work, we assume instead that it is important to identify the strategic actions or behaviors (vital interests) that pose a risk to the home country and its partners and then examine how the gray zone activities contribute to the strategic actions or behaviors that need to be deterred. This argues the need to put the gray zone activities in a strategic context, recognizing that the concern for home country and partner decision makers is that the gray zone activities may collectively lead to an undesirable behavior.

A key issue in deterring gray zone operations is identifying the real intent of the gray zone actor. Often, the actor deliberately introduces ambiguity regarding his intent. Ambiguity and intent are discussed in Section 2. One of the ways that has proven effective in the past to understand other actors is through narrative analysis. This study was informed by a framework developed by Cobb et al.[2] In general, the approach analyzes the other actor's narrative in the context of an action or behavior to be deterred, and then examines the utility of home country and partner actions in terms of how they either reinforce or counter the narrative. Where insights into an actor's doctrine exists, this information can help to put the narrative into context. Examples include the Gerasimov Doctrine (Russia) and publications on China's "Three Warfares."

This approach to deterrence goes beyond just punishment in response to an action. Instead, it adapts the US Department of Defense Deterrence Operations Joint Operating Concept (DO-JOC)[3] to assess the decision calculus surrounding a strategic activity and then considers influence levers to include: impose

1   ELDER, R. J., LEVIS, A. H., and YOUSEFI, B. "Alternatives to Cyber Warfare: Deterrence and Assurance." In JAJODIA, S., SHAKARIAN, P., SUBRAHMANIAN, VS., SWARUP, V., and WANG, C. (eds.) Cyber Warfare – Building a Scientific Foundation, Heidelberg: Springer, 2015.

2   COBB, S., LAWS, D., and SLUZKI, C. "Modeling Negotiation Using 'Narrative Grammar': Exploring the Evolution of Meaning in a Simulated Negotiation." Group Decision and Negotiation, Heidelberg: Springer, February 2013.

3   DO-JOC Deterrence Operations Joint Operating Concept Version 2.0; December 2006 – www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.

punishment, deny benefits of action, reduce cost of not taking action, provide benefits for not taking action, and shift action leverage point in favor of inaction (See section 3). It is important to recognize that actions to deter are situation dependent, and that there are situations where it may be in a state (or other actor's) "national" interest for actions to be executed. This is why the cost-benefit analysis of not acting is a critical element of the decision calculus analysis and is a key area where escalation control principles can provide useful insights.

With the actor and environment established, the next step is to define for each specific actor the potential goals or objectives that the home country wants to deter. Planners will then have all components of the deterrence definition (Section 3) and can then focus on identifying the causal influences contributing (or opposing) the conduct of actions or behaviors that would affect these identified vital home country strategic interests. Examples of strategic interest to deter include occupation of partner territory, creation of humanitarian crises, conflicts that could lead to use of weapons of mass destruction (WMD), or proliferation of technologies that could put WMD in the hands of unstable actors. These strategic interests are not all inclusive, and will vary by international actor.

The next step is to examine those actions from a cause-effect perspective and to identify potential home country responses from an escalation perspective to set the stage for modeling the shaping, engagement, and response activities that should be considered to reduce the risk of the adverse strategic action or behavior occurring. This can be modeled using a Timed Influence Net (Ref) as described in Section 4.

The focal points of this work were (1) the applicability of escalation principles to gray zone actions, (2) the potential utility of non-military instruments of power to counter gray zone activities or increase partner capacity to counter gray zone activity; (3) opportunities to sensitize or counter efforts to desensitize home country and international communities to gray zone activities, (4) potential to reduce ambiguity by contrasting messages and actions to discern objectives, and (5) command and control of non-military elements of power by gray zone actors. While the specific analysis effort was based on gaining an understanding of the decision calculus used by Russia and other relevant international actors relative to actions and behaviors that would be considered adverse by the United States, NATO, and other U.S. partner nations, the description and applicability of the approach is much more general and has been described as such. Finally, conclusions and recommendations are given in Section 5.

ON AMBIGUITY AND INTENT

Ambiguity is defined as the quality of being open to more than one interpretation (Oxford Dictionary) or as a situation or statement that is unclear because it can be understood in more than one way (Cambridge dictionary). In gray zone operations one has to deal with incomplete and often deliberately misleading data at any instant of time. Consequently, ambiguity arises. Ambiguity in the gray zone context means that there can be alternative interpretations regarding what the data represent. It is not a question of uncertainty modeled by probabilities. The explicit consideration of ambiguity helps to nuance some of the gray zone issues.

However, it is intent, not the means that primarily distinguishes gray zone conflicts from other types of conflict. When the general definition of intent is the expression of one's intention or purpose, the military definition is a statement by the commander that succinctly describes what constitutes success for an operation and includes the operation's purpose and the conditions that define the end state. Depending on the intent, one may want the effect of the Gray Zone operations to be observable or the operation to be unobserved/clandestine and not relatable to the effect.

Let us consider two different situations: operations against a financial institution and operations against a government agency. Then the question arises: Why would one target a financial institution or why would one target a government agency? What would the intent be in each case? For the financial institution, one can conjecture that a profit motive would reign high (intent: financial gain); other motives may be to disrupt the markets of the target state, or to undermine a competitor. For the government agency, the intent may be: espionage; terrorism; profit (selling of sensitive the data); bragging rights; or even revenge. Consequently, ambiguity in the intent is one of the more challenging attributes of gray zone operations.

DECISION CALCULUS AND ESCALATION CONTROL

Decision Calculus
In the past, operational planning has focused primarily on developing concepts to defeat a potential adversary militarily. However, such an approach does not always satisfy political requirements. An alternative approach to influence the decision calculus of key regional actors was developed by the US Department

of Defense based on the Deterrence Operations Joint Operating Concept. The concept which underlies this approach was named the Decision Calculus Construct (fig. 1).
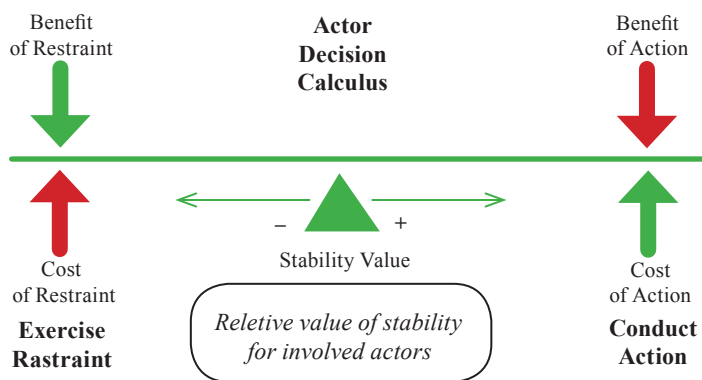
Adapted from Deterrnce Operations Joint Operations Concept (DO–JOC)

Figure 1.
Decision Calculus Construct with Influence Levers

Figure 1 depicts a balance between two activities: Conduct (Adverse) Action and Exercise Restraint (from taking Adverse Action). It is assumed that a home country's Commander's intent is to shift the balance towards Restraint (from Adverse Actions) on the part of all the regional actors who are conducting gray zone operations against the home country or its partners.

The four influence vectors and the fulcrum reflect the perceptions of the actor performing the decision calculus. On the Conduct Action side of the balance are two opposing influences — Benefit of Action and Cost of Action. This is the traditional understanding of deterrence which stressed *imposing cost* (in response to an action) and *denying benefit* of action as a means of deterring adverse behaviors. On the Restraint side of the balance are two influences – *cost of restraint* and *benefit of restraint* (not conducting the adverse activity). A potential perceived cost of restraint is that a government will lose power or face domestically, with partners, or with competitors. Potential benefits could come from the international community or regional actors in the form of economic, political, or social advantages derived from the exercise of restraint.

The fifth, and perhaps most overlooked influence vector expressed in fig. 1 as the fulcrum, is the Regional Actor's perception of the competitor's decision calculus. The Regional Actor's perception can tilt the balance toward Action

(such as to gain advantage by acting first), or toward Restraint (when the competitor's likely proactive course of action is less onerous as the likely response course of action).

The DO-JOC posits that an actor must make cost-benefit decisions to either conduct an adverse action or exercise restraint. The central idea is to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against home country vital interests. This is the objective of joint operations designed to achieve deterrence. For purposes of this study, the central idea is to influence actor behaviors to support strategic geopolitical interests of the home country and its partners. The specific behaviors examined during this study were Russian incursions into neighboring countries due to escalation of tensions between those countries' governments and populations sympathetic to Russia, proliferation of weapons of mass destruction to Russian clients, and strategic miscalculation leading to nuclear weapon use.

Understanding how these factors are interrelated is critically important to determining how best to influence the decision-making calculus of adversaries. Success is not solely a function of whether adversaries perceive the costs of a given course of action (COA) as outweighing the benefits.   Rather, adversaries weigh the perceived benefits and costs of a given course of action in the context of their perceived consequences of restraint or inaction. For example, deterrence can fail even when adversaries perceive the costs of acting as outweighing the benefits of acting if they believe the costs of inaction are even greater.

Joint military operations and activities traditionally contribute to the objective of deterrence by affecting the adversary's decision calculus elements in three ways: Deny benefits, impose costs, and encourage restraint. However, military capabilities can also enable other US and partner instruments of power to be more effective. This is called "Unified Action" of which "Whole of Government" operations are a subset. Direct military means include force projection, active and passive defenses, global strike (nuclear, conventional, and non-kinetic), and strategic communication, i.e., the alignment of actions with intended message. This is often confused with communication strategy. Enabling means include global situational awareness, command and control, forward presence, security cooperation and military integration and interoperability, and assessment, metrics, and experimentation. Additionally, military planners can be of great assistance to other parts of government by helping them analyze the mission, develop and assess courses of action, and model effects of actions.

The perceived benefits and costs of a given Course of Action (COA) to either conduct an adverse behavior (relative to another actor's perception) or to exercise restraint have two essential elements that influence adversary decision-making. First, each benefit and cost has some relative value to the adversary, (i.e., how much does he perceive he will gain by reaping a given benefit or how much does he perceive he will lose by incurring a particular cost). Second, each benefit and cost has a relative probability estimate associated with it in the mind of the adversary; i.e., how likely does he believe it is that he will reap a given benefit or incur a particular cost by acting or not acting.

One additional factor profoundly influences an adversary's decision calculus: his risk-taking propensity. An adversary's risk-taking propensity affects the relationship between values and probabilities of benefits and costs when in the process of reaching a decision. Risk-averse adversaries will see very low probability but severe costs as a powerful deterrent, while risk acceptant adversaries will discount costs in their pursuit of significant gains.

Finally, an actor's decision calculus may be influenced by his perception of the other actors' decision calculus and the time he believes is available to reach a decision. It is important to note that perceptions are more important to an actor's decision calculus than the actual facts underlying these perceptions. Therefore, the conceptual model assumes that stability increases when the actors assess that each other's decision calculus will favor restraint over adverse action.

Escalation Management Principles

Gray Zone Actor escalation indications were developed by applying escalation principles originally developed for use in evaluating strategic deterrence operations. The following seven principles were extracted and adapted from a draft presentation on "Escalation Management Principles" by Pollack and Boyd.[4]

1. Select initial attacks with care (Initiation): A gradual transition from crisis to war is more likely to lead to uncontrolled escalation than a clear and distinct transition from crisis to war.
2. Exercise restraint, or expect reprisals (Restraint): All else being equal, the availability of greater conventional combat power in theater by one side will reduce the chance that the other side will initiate war.

---

4   POLLACK, J. H. and BOYD, D. G. "Identifying Principles for Escalation Management". Unpublished draft, SAIC, 25. August 2011.

3. Maintain availability of conventional forces (Readiness): All else being equal, the availability of greater combat power by one side will reduce the chance that the other side will initiate war as well as reduce the chance of uncontrolled escalation.

4. Select distinct, easily recognized thresholds (Salience): Limitations on warfare that are quantitative (matters of degree) are more likely to lead to uncontrolled escalation than limitations on warfare that are qualitative (either/or).

5. Undercut the adversary's resolve (Resolve): An actor is more likely to achieve its goals if its adversary perceives that the actor is more interested in the outcome and perceives itself as facing higher costs of war.

6. Consider how actions shape the adversary's expectations (Expectations): Actions that lead to achievement of limited objectives, particularly if more closely related to previous actions are less likely to lead to undesired consequences or uncontrolled escalation.

7. Maintain central decision-makers' ability to carry out different COAs (Flexibility): Survivable decision-making and C2 arrangements are less likely to lead to undesired consequences or uncontrolled escalation.

TECHNICAL APPROACH AND TIMED INFLUENCE NET MODELING

Technical Approach

To address and analyze gray zone operations and their deterrence, analytical workflows were developed based on the use of Timed Influence Net models. These models characterize the decision calculus of selected gray zone actors and inform combatant commander and component planning efforts to develop strategies for their area(s) of responsibility. The approach is described in fig. 2.
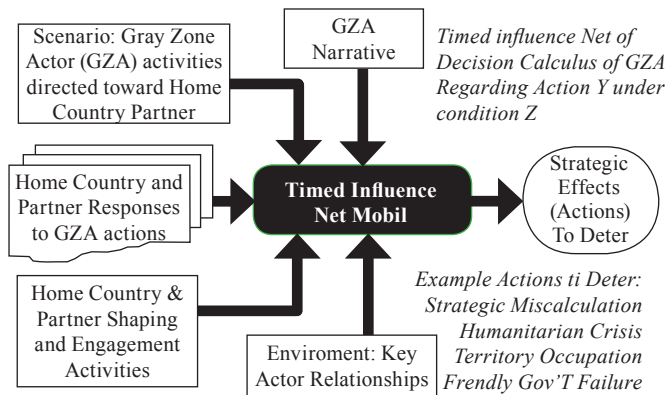
Figure 2.
Schematic depicting the approach for analyzing gray zone operations

Two challenges were addressed using this approach: (a) the need to understand how actions taken by the military or other elements of national power may affect the behavior of a society that includes an adversary and non-adversarial elements, and (b) the need to be able to capture and document data and knowledge about the cultural landscape of an area of operations that can be used to support the understanding of the key issues, beliefs, and reasoning concepts of the local culture so that individuals that are new to the region can quickly assimilate this knowledge and understanding.

The first challenge relates to capabilities that enable the analysis needed to conduct focused effects based planning and effects based operations. Models to support effects based operations developed to date relate actions to effects on the adversary.[5] Such models can be quite effective in informing the comparison of alternative courses of action provided the relationships between potential actions and the effects are well understood. This depends on the ability to model an adversary's intent and his reactions and identifying his vulnerable points of influence. But as the nature of the home country's military operations goes well beyond the traditional major combat operations, there is the need to anticipate the effects of actions not only on the adversary (GZA), but also on the local

---

5   ZAKEM, V., SAUNDERS, P. and ANTOUN, D. "Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union". CNA Occasional White Paper, November 2015.

population which may support or oppose that adversary. Such support may depend in part on the actions taken by the home country.

The second challenge involves the need for new personnel to rapidly assimilate the local knowledge needed to analyze the local situation and to analyze and formulate the effects based plans and operations. Data about a culture exists in many forms and from many sources including historical reference documents, observations and reports by intelligence analysts, and unclassified (and unverified) sources such as the internet. The data is often incomplete and partially incorrect and includes contradictions and inconsistencies. Analysts, particularly those new to an area of operation who are responsible for formulating courses of action, are hard pressed to quickly develop the necessary understanding of the cultural factors that will affect the behavior of the adversary and the society in which it is embedded.

Timed Influence Nets

Several modeling techniques are used to relate actions to effects. With respect to effects on physical systems, engineering or physics based models have been developed that can predict the impact of various actions on systems and assess their vulnerabilities. When it comes to the cognitive belief and reasoning domain, engineering models are much less appropriate. The purpose of affecting the physical systems is to convince the leadership of an adversary to change its behavior, that is, to make decisions that it would not otherwise make. However, when an adversary in imbedded within a culture and depends upon elements of that culture for support, the effects of physical actions may influence not only the adversary, but the individuals and organizations within the culture that can choose to support, be neutral, or oppose the adversary. Thus, the effects on the physical systems influence the beliefs and the decision making of the adversary and the cultural environment in which the adversary operates. Because of the subjective nature of belief and reasoning, probabilistic modeling techniques such as Bayesian Nets and their influence net cousin have been applied to these types of problems. Models created using these techniques can relate actions to effects through probabilistic cause and effect relationships. Such probabilistic modeling techniques can be used to analyze how the actions affect the decision calculus of the adversary.

Influence Nets (IN) and their Timed Influence Nets (TIN) extension are abstractions of Probabilistic Belief Nets also called Bayesian Networks

(BN).[6] BNs and TINs use a graph theoretic representation that shows the relationships between random variables. Influence Nets are directed acyclic Graphs where nodes in the graph represent random variables, while the edges between pairs of variables represent causal relationships. A key differences between Bayesian Networks and INs and TINs is that the letter two use CAST Logic[7] a variant of Noisy-OR,[8] as a knowledge acquisition interface for eliciting conditional probability tables. The modeling of the causal relationships in TINs is accomplished by creating a series of cause and effect relationships between some desired effects and the set of actions that might impact their occurrence in the form of an acyclic graph. The actionable events in a TIN are drawn as root nodes (nodes without incoming edges). Generally, desired effects, or objectives the decision maker is interested in, are modeled as leaf nodes (nodes without outgoing edges). In some cases, internal nodes are also effects of interest. Typically, the root nodes are drawn as rectangles while the non-root nodes are drawn as rounded rectangles. Figure 3 shows a partially specified TIN. Nodes B and E represent the actionable events (root nodes) while node C represents the objective node (leaf node). The directed edge with an arrowhead between two nodes shows the parent node promoting the chances of a child node being true, while the roundhead edge shows the parent node inhibiting the chances of a child node being true. In Figure 3, there is a triplet associated with each link. The triplet is defined a ($\mathbf{h}$, $\mathbf{g}$, t). Parameter $\mathbf{h}$ is the influence that a parent node will have on the child node, if the parent node is TRUE. Parameter $\mathbf{g}$ is the influence the parent node will have on the child node if

6   WAGENHALS, L. W., SHIN, I. and LEVIS, A. H. "Course of Action Development and Evaluation," Proc. 2000 Command and Control Research and Technology Symposium, Naval Postgraduate School, Monterey, CA, June 2000 and WAGENHALS, L. W. and LEVIS, A. H. "Modeling Effects-Based Operations in Support of War Games," Proc. of SPIE, Vol. 4367, Enabling Technologies for Simulation Science V, SISTI, A. F. and TREVISANI, D. A. (eds) Orlando, FL, April 2001.

7   WAGENHALS, L. W., REID, T. J., SMILLIE R. J. and LEVIS, A. H. "Course of Action Analysis for Coalition Operations," Proc. 6th International Symposium on Command and Control Research and Technology, Annapolis, MD, June 2001. and HAIDER S. and LEVIS, A. H. "Dynamic Influence Nets: An Extension of Timed Influence Nets for Modeling Dynamic Uncertain Situations". Proc. 10th International Command and Control Research and Technology Symposium, Washington DC, June 2005.

8   HAIDER, S., ZAIDI, A. K. and LEVIS, A. H. "Identification of Best Sets of Actions in Influence nets," Proc. 2006 Command and Control Research and Technology Symposium, San Diego, CA, June 2006. and WAGENHALS, L. W. and LEVIS, A. H. "Course of Action Analysis in a Cultural Landscape Using Influence Nets, "Proc. IEEE Symp. On Computational Intelligence for Security and Defense Applications, Honolulu, HI, April 2007.

the parent node is FALSE. The third parameter, t, indicates the time delay associated with this link. For instance, event B, in Fig. 3, influences the occurrence of event A after 5 time units.
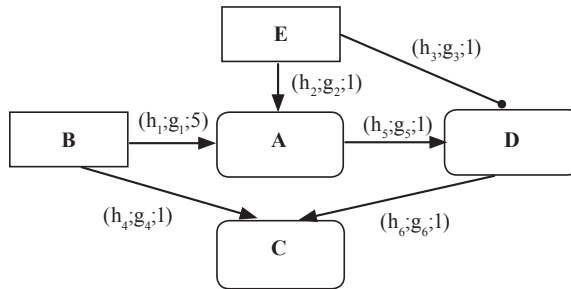
Figure 3.
An Example Timed Influence Net (TIN).

The purpose of building a TIN is to evaluate and compare the performance of alternative courses of actions. The impact of a selected course of action on the desired effects is analyzed with the help of a probability profile. Consider the TIN shown in fig. 3. Suppose the following input scenario is decided: actions B and E are taken at times 1 and 7, respectively. Because of the propagation delay associated with each arc, the influences of these actions impact event C over a period of time. As a result, the probability of C changes at different time instants. A probability profile draws these probabilities against the corresponding time line. The probability profile of event C is shown in fig. 4.
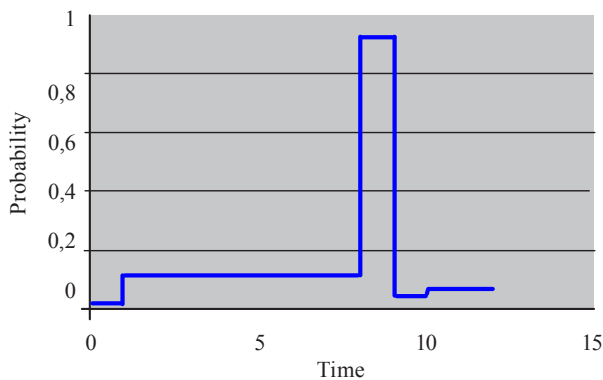
Figure 4.
Probability Profile for Node C

To construct and use a TIN to support the determination of courses of action to deter gray zone operation by an adversary, the following process has been defined.

1. Determine the set of desired and undesired effects expressing each as declarative statement that can be either true or false. For each effect, define one or more observable indicators that the effect has or has not occurred.
2. Build an IN that links, through cause and effect relationships, potential actions to the desired and undesired effects. Note that this may require defining additional intermediate effects and their indicators.
3. Use the IN to compare different sets of actions in terms of the probability of achieving the desired effects and not causing the undesired effects.
4. Transform the IN to a TIN by incorporating temporal information about the time the potential actions will occur and the delays associated with each of the arcs and nodes.
5. Use the TIN to experiment with different timings for the actions to identify the "best" COA based on the probability profiles that each candidate generates. Determine the time windows when observation assets may be able to observe key indicators so that assessment of progress can be made during COA execution.
6. Create a detailed execution plan to use the resources needed to carry out the COA and collect the information on the indicators.
7. Use the indicator data to assess progress toward achieving the desired effects.
8. Repeat steps 2 (or in some cases 1) through 7 as new understanding of the situation is obtained.

To analyze the TIN (Step 5), the analyst selects the nodes that represent the effects of interest and generates probability profiles for these nodes. The probability profiles for different courses of action can then be compared.

An Illustrative Example

One scenario that was of particular interest was a situation where a gray zone actor would shift from competition short of armed conflict to a more aggressive stance where occupation of a competitor's territory came under consideration. The specific scenario was one in which a large percentage of the targeted country's population was of the same ethnicity as the gray zone actor, and a perception existed among the gray zone actor's population that this ethnic minority was not being treated properly by the targeted country. The gray

zone actor in the scenario possesses a much more powerful military capability and is significantly larger than the targeted country in economic terms. On the other hand, the target country does enjoy a favorable relationship with the European Union and the US. A Timed Influence Net model (fig. 5) was developed using the software application Pythia[9] (Levis, 2014) to examine the factors that would be involved in the decision calculus of the gray zone actor, postulate how the gray zone actor might set the conditions for taking military action, and consider opportunities for the country targeted for occupation or its allies to influence the gray zone actor's decision calculus.
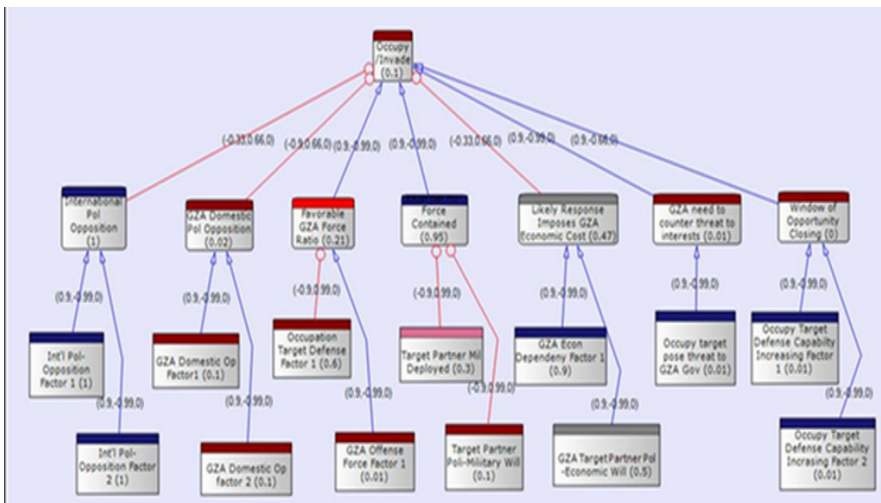
Figure 5.
The TIN model for the example scenario

Although there could be many factors involved in the gray zone actor's decision calculus relative to the decision to occupy territory of another country, seven primary factors using the decision calculus framework were identified. These factors are:
International political opposition;
    Gray zone actor domestic population opposition;
    The ratio of the gray zone actor force to target country force;
    The ability to contain external forces from supporting the target country;

9   LEVIS, A. H. "Pythia User's Manual, v. 1.803". System Architectures Laboratory, George Mason University, 2014.

The impact of the potential economic response to the occupation;

The gray zone actor's perception of the need to occupy the targeted country to counter threats to national interests; and

The gray zone actor's perception that the window of opportunity to conduct the invasion was closing.

Numerous variations of unopposed and opposed courses of action were considered, but only two will be highlighted here. In the first course of action (unopposed), the gray zone actor is able to establish a positive balance of power both militarily and politically with very little tangible opposition from the countries allied to the targeted country. By the time the target country's allies realize that adverse action on the part of the gray zone actor is imminent, it is too late to prevent the occupation from taking place. This is depicted graphically in Fig. 6. In the second course of action (opposed), also in Fig. 6, once it becomes clear to the target country and its partners that the gray zone actor perceives the need to counter a threat to its interests from the targeted country, the targeted country and its partners implement a strategy of political, economic, and military actions to influence the gray zone actor's decision calculus to adapt a more acceptable behavior to the international community.   The comparison figure illustrates the difference in the invasion decision calculus when the gray zone actor's actions are unopposed versus a course of action where the gray zone actor's actions are opposed by the target country's partners.
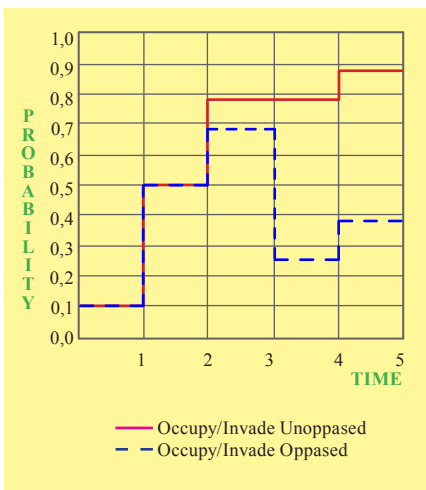
Figure 6.
Probability of Gray Zone Actor achieving the occupation goal when opposed and when not opposed by target country's allies

Figures 7 and 8 depict the probability profiles of the unopposed and opposed course of actions in more detail and illustrate the impact of the primary factors on the decision calculus of the gray zone actor.
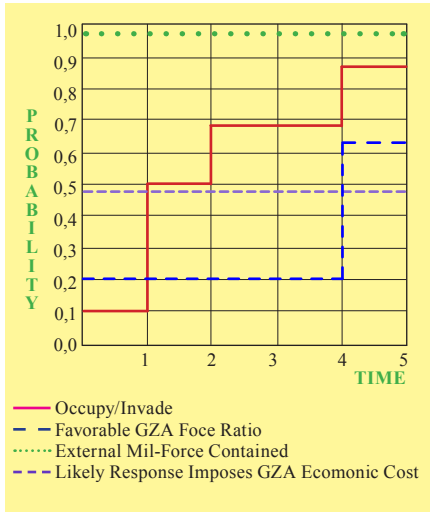
Figure 7.
Unopposed Occupation
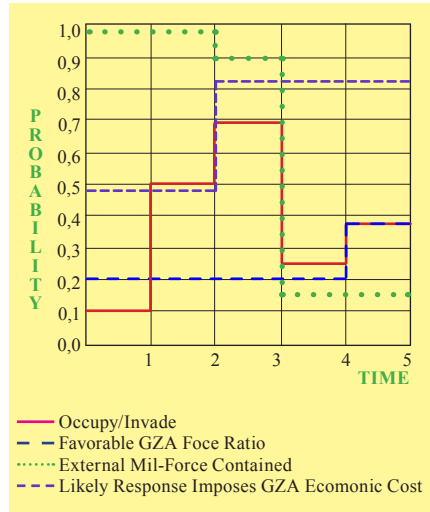
Figure 8.
Opposed Occupation

The Deterrence Workflow

Since the purpose of this work is to arm planners with a framework they can use for planning home country and partner activities to deter actions or behaviors adverse to home country interests, the overall approach for assessing potential home country and partner actions relative to competitors from an escalation perspective is shown in Fig. 9. This approach serves as a tool to provide insights into the freedom of maneuver available to each actor, and identify capabilities a home country needs to counter its own gray zone challenges capability gaps.
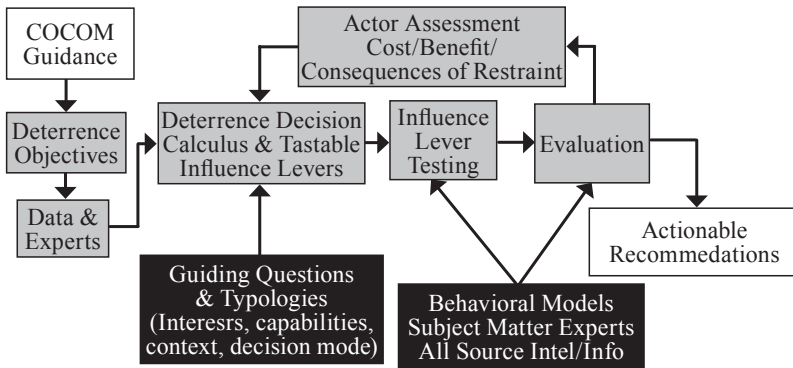
Figure 9.
Operationalizing Deterrence Workflow

Conclusions

While the original focus was on gray zone activities, it was useful to address the gray zone activities of all actors that are involved competition short of armed conflict or possible precursors for military action. For this reason, it was useful to reduce ambiguity by assessing the actions and messages of the gray zone actor in the context of the competing interests between the gray zone actor and the gray zone target country and its partners. Assessing the gray zone activities in the context of strategic competition provided insights into the objectives of the gray zone actor relative to the target country.

Applying escalation principles to gray zone actions provided insights into the gray zone actor's strategy to influence the potential response from the gray zone target's partners. For example, escalating the competition slowly leads over time to a shift in the baseline of activities the gray zone partners accept as "normal" competition. This is an application of the initiation and salience principles. Analysis from experiments conducted using the Timed Influence Net models suggests that a gray zone actor can position itself to achieve its objectives with little opposition through application of the escalation principles of readiness and resolve.

Although the decision calculus framework did not seem effective as a means to counter individual gray zone activities, largely because it is difficult to deter a behavior that is considered normal competition, it can be an effective means to counter the ultimate objective that the gray zone activity is intended to

support. We found the decision calculus framework to be useful operationally as a means to examine opportunities to restore or maintain stability in the face of gray zone actor activity which could lead to detrimental outcomes from the perspective of the home country.

The decision calculus framework can also be used to counter efforts to desensitize home country and international communities to the gray zone activities. A home country wants the gray zone actor to perceive that the home country and partners will understand the intended effect of a gray zone action when that effect is adverse to its interests. They also want the gray zone actor to expect them to respond to the gray zone activities either by denying the benefits of the action or imposing an unacceptable cost. On the other hand, a gray zone actor perceives that the home country is most likely to avoid escalating the situation and pursue a "least cost" solution both economically and politically, particularly if the gray zone actor is successful in maintaining ambiguity regarding the intended effects of the actions. The decision calculus framework can be used to (1) understand the gray zone actor's efforts to limit the host nation's response flexibility; (2) develop host nation strategies to limit the gray zone actor's options, (3) promote the benefits of de-escalation, and (4) identify other influence levers such as relevant costs the host nation can impose.

Finally, gray zone actors must often find means to influence the actions of non-military elements of power that are not under their direct control. This requires the ability to control the information that its citizens and partners receive. Since many gray zone actor governments control the media and access to social media, gray zone activity command and control can be difficult for a gray zone target country or its partners to counter. For this reason, a host nation will likely find it more effective to counter the gray zone actor's objectives and overall strategy rather than attempt to counter individual activities. In this way, traditional counter command and control strategies can be exercised.

Lieutenant General Robert Elder (USAF, retired) joined the George Mason University faculty as a research professor with the Volgenau School of Engineering following his retirement from military service as the Commander of 8th Air Force and U.S. Strategic Command's Global Strike Component. He currently conducts research in the areas of command and control, deterrence, escalation control involving international

competition short of armed conflict, crisis management, and international actor decision-making. He received his Doctorate in Engineering from the University of Detroit.

Dr. Alexander H. Levis is University Professor of Electrical, Computer, and Systems Engineering in the Volgenau School of Engineering, George Mason University. From 2001 to 2004 he served as the Chief Scientist of the US Air Force. He was educated at Ripon College where he received the AB degree (1963) in Mathematics and Physics and then at MIT where he received the BS (1963), MS (1965), ME (1967), and Sc.D. (1968) degrees in Mechanical Engineering. He is a Fellow of IEEE, INCOSE, AAAS and Assoc. Fellow of AIAA. For the last fifteen years, his areas of research have been system architecture design and evaluation, resilient architectures for command and control, and evaluation of cyber exploits on system behavior. He can be reached at alevis@gmu.edu.

BIBLIOGRAPHY

COBB, S., LAWS, D., and SLUZKI, C. "*Modeling Negotiation Using 'Narrative Grammar': Exploring the Evolution of Meaning in a Simulated Negotiation*" Group Decision and Negotiation, Springer, February 2013

DO-JOC Deterrence Operations Joint Operating Concept Version 2.0, December 2006 – www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.

ELDER, R.J., LEVIS, AH, and YOUSEFI, B. *"Alternatives to Cyber Warfare: Deterrence and Assurance*" In JAJODIA, S., SHAKARIAN, P., SUBRAHMANIAN, VS., SWARUP, V., and WANG, C. (eds.) *Cyber Warfare – Building a Scientific Foundation,* Heidelberg, Springer, 2015.

HAIDER S. and LEVIS, A. H. "*Dynamic Influence Nets: An Extension of Timed Influence Nets for Modeling Dynamic Uncertain Situations*" Proc. 10th International Command and Control Research and Technology Symposium, Washington DC, June 2005.

HAIDER, S., ZAIDI, A. K. and LEVIS, A. H. "*Identification of Best Sets of Actions in Influence nets*" Proc. 2006 Command and Control Research and Technology Symposium, San Diego, CA, June 2006.

LEVIS, A. H. "*Pythia User's Manual, v. 1.803*". System Architectures Laboratory, George Mason University, 2014.

POLLACK, J. H. and BOYD, D. G. "*Identifying Principles for Escalation Management*" Unpublished draft, SAIC, 25. August 2011.

WAGENHALS, L. W. and LEVIS, A. H. Course of Action Analysis in a Cultural Landscape Using Influence Nets, Proc. *IEEE Symp. On Computational Intelligence for Security and Defense Applications,* Honolulu, HI, April 2007.

WAGENHALS, L. W. and LEVIS, A. H. "*Modeling Effects-Based Operations in Support of War Games*" Proc. of SPIE, Vol. 4367, Enabling Technologies for Simulation Science *V,* SISTI, A. F. and TREVISANI, D. A. (eds) Orlando, FL, April 2001.

WAGENHALS, L. W., REID, T. J., SMILLIE R. J. and LEVIS, A. H. "*Course of Action Analysis for Coalition Operations*" Proc. 6th International Symposium on Command and Control Research and Technology, Annapolis, MD, June 2001.

WAGENHALS, L. W., SHIN, I. and LEVIS, A. H. "*Course of Action Development and Evaluation*" Proc. 2000 Command and Control Research and Technology Symposium, Naval Postgraduate School, Monterey, CA, June 2000.

ZAKEM, V., SAUNDERS, P. and ANTOUN, D. "*Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union*" CNA Occasional White Paper, November 2015.

Krisztián Jójárt and András Rácz
Contemporary Russian Military Thinking on Conflicts of the 21st Century: Beyond the 'Gerasimov Doctrine'

Abstract: The paper provides an overview of how armed conflicts of the 21st century are perceived in contemporary military thinking of the Russian Federation. The main question we intend to answer is to what extent Russian military thinking on contemporary conflicts has changed since Chief of General Staff Valery Gerasimov has published his landmark article, widely known as the "Gerasimov doctrine," in the *Voenno-promishlenniy kurier* in 2013. More concretely, what effects the experiences gained from the war in Ukraine and in Syria have had on contemporary Russian military thinking.

The analysis provides an overview of the state of Russian military thinking on the nature of armed conflicts at the time Gerasimov's article was published, it studies the discourse since then, and also applies a "reality check:" a comparison of the scenarios of the Russian military exercises with the ongoing theoretical discourse.

Forerunners of the Gerasimov Doctrine

Russian military thinking has at least a century-long, nearly uninterrupted tradition, dating back at least to the early years of the Soviet Union. While the post-Soviet transformation deprived the military most of its earlier resources, theoretical work on the nature and characteristics of war was not interrupted. There has been a lot of continuity both in terms of institutions, personnel and also fora of publication. Moreover, post-Soviet Russian military thinkers keep monitoring the works of their foreign counterparts, let them be from the West or China, and keep assessing the effects of these developments for Russia. In other words, Russian military science is not developing in isolation,

it is actively following, reflecting and further developing concepts, ideas and lessons learnt by foreign militaries from their wars.

For example, in his book published in 1995, Russian General Makhmut Gareev[1] discussed in detail the characteristics and nature of future war, into which he already factored the experiences of the U.S. campaign against Saddam Hussein. Gareev predicted that technological development, primarily the emergence of long-range artillery and missile systems will make it possible to swiftly penetrate the whole depth of enemy territory. He also forecast that non-kinetic components of war, primarily cyber and information warfare will play a key role in future armed conflicts, and technological developments will make them a lot more advanced than they were in Gareev's times.

Major-General Vladimir Slipchenko wrote extensively about the coming sixth-generation warfare already in the 1990s, further developing Gareev's theories as well. Slipchenko's logic was based on the changing characters of weaponry and on the shift from one generation of weapons to the next one.[2] According to Slipchenko, technological development will make it possible for a sixth-generation war to be a "non-contact" one, when long-distance strikes will come from space, from the air and also from computer systems, without the need to actually put boots on the ground. The military, political and economic targets of the enemy, with particular emphasis on the command and control infrastructure, could be destroyed without engaging the enemy in a conventional attack.[3] The changes in Russian military thinking about the nature of future war, including the increased importance of high-precision weapons, in-depth strikes, long-range fire combat, as well as of information warfare, were also reflected in a White Paper published in 2003.[4]

In the mid-2000s, Russian scholars studied extensively the lessons of the wars in Iraq and Afghanistan, the so-called 'color revolutions' of the post-Soviet space, as well as events of the Arab Spring. Particularly the latter have been widely perceived in Russia as plots orchestrated by the West through

---

1   GAREEV, M. If War Comes Tomorrow? The Contours of Future Armed Conflict. Translated by Yakov Vladimirovich Fomenko. Abingdon: Routledge, 1998.

2   THOMAS, T. Thinking Like a Russian Officer. Basic Factors and Contemporary Thinking on the Nature of War. Fort Leavenworth: Foreign Military Studies Office. April 2016; p. 4.

3   MATTSON, P. "Russian operational art in the fifth period: Nordic and Arctic applications." Revista de Ciências Militares, Vol. 1, N.º 1, May 2013 – http://www.iesm.pt/cisdi/revista/Artigos/Revista_1_Artigo_1.pdf – p. 29–47.

4   RÁCZ, A. Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist. Helsinki: The Finnish Institute of International Affairs. June 16., 2015 – http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine/ Accessed on June 27., 2017; p. 36.

mobilization of the societies, by using information warfare, propaganda and special operations means, leading to the conclusion that the importance of non-military tools in achieving political aims has been increasing significantly.

All in all, the well-known, already famous article of Gerasimov[5] has not appeared as a revolutionary novelty or unexpected intellectual leap. Instead, it was the result of a long, evolutionary development process. The reasons why it has caused such a surprise and revelation in the West following the annexation of the Crimea are to be found not in Russia itself, but in the earlier negligence and indifference of the West towards Russian military thinking.

THE "GERASIMOV DOCTRINE"

Chief of the Russian general staff, Valeriy Gerasimov is widely regarded in the West as the father of Russia's hybrid warfare since his landmark article was discovered, translated and circulated by Robert Coalson in June 2014. At this time the world has already seen the annexation of Crimea and was closely watching the events taking place in Eastern Ukraine. As there was a close logical correlation between General Gerasimov's article[6] published in February 2013 and the operation in Crimea and Eastern Ukraine, many widely accepted Gerasimov's writing as the hybrid warfare doctrine of the Russian Armed Forces. However, among experts the interpretation of Gerasimov's article is a subject of debate to this day. This is due to the fact that the article is far from being a user's manual for hybrid warriors and its text is formulated in a way to purely provide a description of today's war through the examples of – real or perceived – Western military operations. The presentation of the Arab Spring by Gerasimov as a covert Western operation is regarded by Mark Galeotti and others as "an old Soviet-era rhetorical device" to hide the true intention of the article, namely to introduce "how Russia can subvert and destroy states without direct, overt and large-scale military intervention."[7]

---

5   See Robert Coalson's Twitter post with reference to the translated article here: Robert Coalson's twitter post. Twitter. June 21., 2014 – https://twitter.com/coalsonr/status/480374222997692416 Accessed on June 27, 2017.

6   GERASIMOV, V. "Tsennosti nauki v predvidenii." [The Value of Science in Prediction] Voyenno-Promishlenniy Kurer. February 27., 2013 – http://www.vpk-news.ru/articles/14632 Accessed on June 27., 2017.

7   GALEOTTI, M. "The 'Gerasimov Doctrine' and Russian Non-Linear War." In Moscow's Shadows [blog] July 6, 2014 – https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ Accessed on June 27., 2017.

Other analysts argue for the reading of Gerasimov literally, i.e. to interpret Gerasimov's words as they are. Roger McDermott puts the article in context and claims that Gerasimov's motive was to resurrect the independent Russian military academic thinking. He believes Gerasimov's article is nothing close to a doctrine[8] and was only meant to be a call for debate by playing on the strings of fear from the repeat of surprise attack a similar ti the June 1941 German invasion.[9] Charles Bartles underlines the very same circumstance behind the birth of the article. Bartles also emphasizes that interpreting color revolutions and the Arab Spring as a U.S. covert operation might sound weird for Western audience, in Russian narrative the fear from an American-ignited regime change or Yugoslavia-like dissolution is genuine.[10] This paper's authors are also convinced that this reading of the Arab Spring is truly and widely regarded as factual among the Russian people as well as the elite, and that Moscow frankly fears a US-orchestrated regime change. This, however, does not rule out the possibility that Gerasimov also intended to to call for balancing of the perceived threat by applying the same tools as the potential adversary. It is enough to think on Russian worries about Western media dominance and how Russia aimed to counter it by establishing a CNN look-alike television channel, the RT.

What Gerasimov claims foremost in his article is that the line between war and peace is blurred. This statement has a clear significance as some of the measures (mostly non-military ones) of the new generation of war are applied even before the recognized divergence of interests between the conflicting parties, let alone the period of open conflict.[11] Among them are strategic containment, the formulation of coalitions and alliances, the creation of political opposition, and – most importantly – the information operations which are present in every phase of the conflict. The aim is not the physical destruction of the enemy forces and infrastructure, but to break the resistance and morale of the population and ability of the target country to resist. In the achievement of that non-military measures often have a greater importance

---

8   This does not contradict Galeotti's opinion, who also acknowledges the unfortunate spread of the expression 'Gerasimov doctrine' due to the "snappy title" of his blog post. Ibid.

9   McDERMOTT, R. N. "Learning From Today's Wars. Does Russia Have a Gerasimov Doctrine?" in Parameters. Spring, 2016 – https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2016/12_McDermott.pdf Accessed on June 27., 2017; p. 99–100.

10   BARTLES, C. K. "Getting Gerasimov Right." in Military Review. January-February, 2016 – http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf Accessed on June 28., 2017.

11   GERASIMOV. "Tsennosti nauki v predvidenii."

than traditional military ones. Accordingly, Gerasimov determines the ratio of military and non-military measures as 1:4.[12] The offender party relies on a wide range of tools, including information operations and the use of numerous proxy actors, such as local opposition forces and private military companies. Special operation forces – which are not regarded by Gerasimov as a military measure – also play a key role in achieving the war aims. The use of conventional armed forces is restricted only to the achievement of the final success often in the form of a peacekeeping mission.[13]

The fact that Gerasimov has not been a lone revolutionary thinker is reflected by a nearly prophetic article of two well-known Russian military theorists, Sergey Chekinov and Sergey Bogdanov. In their piece published in December 2013[14] they outlined a detailed, step-by-step roadmap of a "new generation war." In other words, they basically operationalized the general idea laid out by the Chief of the General Staff. By continuing the defensive narrative, Chekinov and Bogdanov stressed the asymmetric nature of future armed conflicts, thus wrote explicitly about how non-military tools and means are going to be employed by the attacker. They go into such depth of detail as listing even the foreseeable actions of religious organizations, cultural institutions, NGOs, public movements financed from abroad, and scholars engaged in research on foreign grants, as possible components of a coordinated attack against the target country. The Russian attack on Ukraine that took place a few months later reflected their vision with extraordinary accuracy.

CURRENT RUSSIAN THEORIES
ON THE WAR OF THE FUTURE

The methods Russia used during the occupation of Crimea and the war in Eastern Ukraine had caught the West by surprise. However, the main lesson that can be drawn from the war in Ukraine is that the theory of the so-called hybrid warfare was present in open sources well before the war, in the publications of Russian military thinkers. Now that the world has already paid considerable attention to Gerasimov's study on the war of the future,

---

12   Ibid.
13   GALEOTTI. "The 'Gerasimov Doctrine.'"
14   CHEKINOV, S. – BOGDANOV S. "The Nature and Content of a New-Generation War." Military Thought, October-December 2013 – http://www.eastviewpress.com/Files/ MT_FROM%20 THE%20CURRENT%20ISSUE_No.4_2013.pdf Accessed on June 27., 2017; pp. 12–23.

and Bogdanov's and Chekinov's detailed 'guidebook' of hybrid warfare, it is about time to leave them behind and follow what Russian military theorists are currently thinking about the war of today and tomorrow. Because the other main lesson of Russian warfare is its unpredictability: it is highly unlikely that what we should prepare for in the future is another Ukraine-like hybrid war.

WHAT IS KEEPING THE RUSSIAN MILITARY ELITE AWAKE AT NIGHT?

As opposed to their Western counterparts who have been researching counter-insurgency strategies in the last decades before turning their attention back to Moscow three years ago, Russian military thinkers – while the armed forces waged their own wars with insurgency in Chechnya – have never lost sight of their old enemy, and closely examined military interventions of the NATO and the U.S. from Yugoslavia to Libya. Articles currently published in Russian military journals testify to an extreme level of distrust – if not outright paranoia – toward the U.S. The main concerns attributed to Washington range from regime change and partition of Russia to upsetting strategic parity. The latter challenge is being manifested through the development of high-precision and high-speed global strike capability[15] and the deployment of missile defense systems.[16] Previously, the Russian narrative on the U.S. missile defense deployment emphasized that the system would dangerously undermine Moscow's second strike capability. Today the narrative has changed, and the anti-ballistic missile complexes are now regarded as offensive weapon systems. They are allegedly universal launching platforms, which enable the U.S. to launch offensive high-precision missiles from these sites. The American initiatives to reach an agreement on the further reduction of strategic nuclear capabilities on both sides are also interpreted within such suspicious context.[17]

---

15   BARVINENKO, V. "Ot asteroida i provokatora" [From asteroid and provocateur] in Voyenno-Promishlenniy Kurer. June 7., 2017 – http://www.vpk-news.ru/articles/37129 Accessed on June 27., 2017.

16   VASILYEV, S. – KRIVORUCHKO, V. "Nash nevniatniy otvet agressoru – chast' I." [Our inarticulate response to the aggressor – part one] in Voyenno-Promishlenniy Kurer. May 17, 2017 – http://www.vpk-news.ru/articles/36744 Accessed on June 27., 2017.

17   Ibid.

WHAT WILL THE WAR OF THE FUTURE LOOK LIKE?

High precision, contactless, network-centric

There is another reason Russian military thinkers turn their attention toward the United States. They believe that technology will determine the forms of future war, in line with the already described works of Gerasimov's predecessors, such as Slipchenko. As technological supremacy in the field of defense industry is still in American hands, this practically means that the war of the future will be made in the U.S.A. Consequently, Russian military thinking is in a responsive posture insofar as it closely follows American military developments and the potential challenges for Russia arising from them. At the same time, it critically assesses new advances, both adapts and works hard to counter them by exploiting their weaknesses and by developing asymmetric responses.

Sergey Kiselyev in his article "What Types of War must the Russian Armed Forces be Prepared for" specified two main types of wars for the present and the near future. The first one targets the infrastructure, the political and economic potential of the enemy country while destroying the armed forces only on a minimal level as long as ground intervention is not part of the plan. It was exemplified by the 1999 air campaign against Yugoslavia. The second type aims to grab territory and to establish (or restore) democracy. This is achieved through the destruction of armed forces and the breaking of the morale of the population, while economic potential is left mostly untouched. Kiselyev mentions Operation Desert Storm and the 2003 Iraq War as examples. While the second type of war relies on ground forces to achieve the objective, both types of war start with a contactless period in which precision weapons play the major role.[18] Kiselyev also emphasizes the significance of network-centric approach and the information space as a new domain. He expects an extensive use of cyber-warfare and operations affecting not only the human mind but the sub-consciousness.[19]

The question of how to respond to these developments apparently divide the Russian military thinkers. The authors of a debate-inducing article call for a change in the defensive-oriented approach of the Russian armed forces, as

---

18 KISELYEV, V. A. "K kakim voynam neobhodimo gotovit' Vooruzhennie Sili Rossii." [What Types of Wars must the Russian Armed Forces be Have to Prepared for] in Voyennaya Misl No. 3/2017 March, 2017; p. 37–38

19 Ibid.

in their understanding the current nature of war favors the offender.[20] They believe that Russia spends way too much money on its air and space defense forces to counter American global strike capabilities. According to their reasoning this unintentionally serves U.S. interests, as Washington's constant pursuit for technological breakthroughs is the very heart of a strategy to coerce rival states to turn their resources to defense instead of building up their offensive capabilities.[21] Vladimir Barvinenko, while not disputing this, regards the development of air and space defense forces essential. In his opinion the main lesson of the conflicts after the Second World War is that the U.S. has managed to achieve its goals in those cases when the targeted state lacked effective air defense, while he attributes the failure in Vietnam to the presence of Soviet air defense systems.[22] The political and military leadership also shares this thought, as recent developments suggest.

Besides maintaining high spending levels on air and space defenses, the Russian military elite also aims to raise the ratio of high-tech offensive weapons. General Gerasimov claims that the striking potential of high-accuracy weapons will quadruple in the Russian military by 2021.[23] Another author calls for the creation of the human basis of technological development.[24] All in all, the Russian military elite on the one hand tries to build up defensive capabilities against high precision Western weapons, while on the other hand it pursues the goal to raise the number of such weapons within the Russian military as well.

20   VASILYEV, S. – KRIVORUCHKO, V. "Nash nevniatniy otvet agressoru – chast' II." [Our in-articulate response to the aggressor – part two] in Voyenno-Promishlenniy Kurer. May 24, 2017 – http://www.vpk-news.ru/articles/36878 Accessed on June 27., 2017.

21   VASILYEV– KRIVORUCHKO. "Nash nevniatniy otvet agressoru – chast' I."

22   BARVINENKO, V. "Ot asteroida i provokatora."

23   GERASIMOV, V. "Mir na granyah voyni. Malo uchitivat' sevodniashnee vizovi, nado prog-nozirovat' budushchie." [Peace on the brink of war. Not enough to calculate with challenges of the present, should predict future ones] Voyenno-Promishlenniy Kurer. March 15, 2017 – http://www.vpk-news.ru/articles/35591 Accessed on July 3., 2017.

24   Sergey Pershutkin emphasizes the need to employ mathematicians and physicists in the military. He also mentions the already laid down goal to raise the ratio of personnel with a doctorate de-gree to 60% by 2025 in the subordinate institutions. PERSHUTKIN, S. "Talanti – v kurszanti. Dla oruzhia na novih fizicheskih printsipah nuzhni offitseri-intellektuali i sovietskie metodiki." [The talented – to the military academy. For the weapons based on new physical principles intel-lectual officers and soviet methodos are needed] in Voyenno-Promishlenniy Kurer. June 14., 2017 – http://www.vpk-news.ru/articles/37230 Accessed on June 27., 2017.

Hybrid

Sergey Kiselyev mentions another type of war in his article. The way he describes this type, it is not a war de jure but de facto, "the most productive from a military point of view" as it weakens the enemy and causes tangible losses to them."[25] The same is emphasized by Valeriy Gerasimov who also finds the novelty of this warfare in the fact that it "does not fall under the definition of aggression."[26] Illegal armed groups and private military companies form the basis of this war which aims to either crush the country into multiple small pieces or to separate a territory and establish a new government there.[27] While both authors claim that this is also part of the Western toolset, in reality the description perfectly fits the war seen in Ukraine. There is another reason to believe that both authors actually regard it as a Russian method of asymmetric warfare: cheapness. As Gerasimov put it, the cost of weapons and the war in general has become an important factor choosing the ways to conduct military operations.[28] In Gerasimov's opinion hybrid replaced contactless war.[29]

While the changed nature of war and the growing significance of information space and non-military tools (in the exploitation of which Moscow has undisputable merits) are all acknowledged, armed violence – the main content of war – will still remain a key element of wars in the foreseeable future as believed by Russian military thinkers.[30]

WHAT ARE THE RUSSIAN ARMED FORCES PREPARING FOR? – A CRITICAL ASSESSMENT OF RUSSIAN MILITARY EXERCISES

After the collapse of the Soviet Union more than a decade-long steady decline awaited the Russian armed forces. The shrinking defense budget and the rampant corruption dramatically affected both the technical and the human components of the military. In 1993 then-chief of the general staff, Colonel General Mikhail Kolesnikov, when evaluating the few exercises conducted in the year, talked about "poor command preparation, deficient knowledge

---

25   KISELYEV. "K kakim voynam neobhodimo gotovit' Vooruzhennie Sili Rossii."
26   GERASIMOV. "Mir na granyah voyni."
27   KISELYEV. "K kakim voynam neobhodimo gotovit Vooruzhennie Sili Rossii."
28   GERASIMOV. "Mir na granyah voyni."
29   Ibid.
30   Ibid.

of operational procedures, and an alarming buildup of unserviceable equipment."[31] Due to disastrous shortcomings, Moscow had reintroduced large-scale military training only in 2009 with the Zapad (West) strategic exercise. Since then Russia has consistently increased both the number of exercises and the participating forces. Analyzing these exercises allows us to draw conclusions about the status of the armed forces of the Russian Federation as well as to assume Moscow's foreign policy intentions and perception of security. It should be noted that the military exercises have significance beyond the conventional purpose of training the armed forces and are an important element of Russia's foreign policy toolset. The present analysis describes Russia's military exercises through this lens.

Training
With focus on the conventional training purpose of the military exercises it can be said that the Russian Federation has been preparing for large-scale interstate wars, often with an escalation to the nuclear level.[32] Johan Norberg in his thorough study, which analyzed Russian military exercises between 2011 and 2014, differentiates three types of exercises: strategic exercises, parallel exercises and surprise inspections. One strategic exercise is held in every year covering a major strategic direction including mostly – but not exclusively – forces of the given military district where the exercise is taking place. Parallel exercises are training events conducted in close proximity in time to the strategic exercise and in another, generally adjacent military district. While the exercises are regularly held and planned in months advance, surprise or snap inspections are meant to test the readiness of the armed forces.[33]

While the most spectacular elements of the exercises are beyond doubt the field training exercises, from an expert's point of view the more interesting details lie below the surface. As Norberg concluded, training does not focus solely on the armed forces, but also tests the whole war-waging capacity of the Russian Federation. This includes – besides units of the FSB (Federal Security Service) and Interior Ministry – key departments and ministries of transportation and telecommunication as well.

---

31   LAMBETH, B. S. "Russia's Wounded Military." Foreign Affairs. March/April, 1995; p. 89
32   NORBERG, J. Training to Fight - Russia's Major Military Exercises 2011-2014. Stockholm: FOI. December, 2015 – https://www.foi.se/report-search/pdf?fileName=D:%5CReportSearch%5CFiles%5C8e2dc822-a31c-4f6c-aecd-954375e3fe31.pdf Accessed on June 26, 2017 p. 61.
33   Ibid.

In expert circles probably the most crucial observation as far as the exercises are concerned is the apparent fact that Moscow can move its warfighting assets surprisingly quickly from one part of the country to another via air lift and railway. Consequently, it means that assessing Russia's force projection capabilities toward a given strategic direction by counting the units and equipment permanently stationed within the military district in question is purely wrong. It seems that Moscow is not only able to transport its military units quickly over long distances if necessary, but it clearly regards this capability as a fundamental element of its strategic thinking. This was also proven by the Vostok (East) 2014 exercise, during which strategic air transports from western Russia extended up to 6,000 km's distance.[34] All in all, Moscow likely regards the whole military as a basis of launching operations in any direction as it was underlined during the war in Ukraine as well (see later).

Deterrence, threat and the dark power

In so-called hybrid warfare the threat of conventional military forces has a key significance. In the spring of 2014 Moscow used snap exercises to threaten Kiev with a full-scale conventional war. That exercise which was the sixth surprise inspection of the year involved around 150,000 servicemen and was heavily publicized by the Russian MoD.[35]

Russian military exercises are well communicated and probably serve the secondary function to deter possible adversaries from attacking or pressuring Russia. The fact that the stated official numbers of participants in the exercises has grown six- to eightfold between 2011 and 2014 does not necessarily mean real growth of such a scale but rather a decreasing incentive to present the exercises as smaller than than they actually are. It testifies to Moscow's loss of interest in complying with arms control and security and confidence building measures.[36] These are sacrificed for the sake of complementing the rhetoric of saber-rattling with military might. This is another example of dark power, a notion introduced by Mark Galeotti to describe "the malign shadow of soft power" which meant to accumulate power through fear.[37] This was illustrated recently by the news on the approaching Zapad-2017 exercise. In

---

34   Ibid. p. 45.
35   The event generated 16 articles on the website of the MoD compared to the average 1–2 and a highest number of 11 before. Ibid. p. 50.
36   Ibid. p. 62–63.
37   GALEOTTI, M. "It's the Russians Wot Done It." The Moscow Times. June 20., 2017 – https://themoscowtimes.com/articles/its-the-russians-wot-done-it-58228 Accessed on June 27., 2017.

November 2016 Ukrainian sources noticed a tender announced by the Russian MoD for 4,162 railway wagons for shipments to and from Belarus in 2017.[38] The information was quickly connected to the planned Zapad 2017 exercise and led Lithuanian president, Dalia Grybauskaitė to call it a preparation for war with the West.[39] A number of analysts also concluded that this might be the largest military exercise since 1991 with an estimated 30,000 Russian military personnel deployed to the territory of Belarus.[40] Moscow was not quick to dissipate concerns and clarified the news only two months later upon the request of the newspaper Novaya Gazeta.[41]

Maskirovka

The most worrisome function of Russia's military exercises is to disguise (maskirovat') real military maneuvers. It has already been widely suspected that Russia exploited the Kavkaz exercise to cover its military build-up against Georgia in 2008. In 2014 it was factually proven that Moscow transferred military units to the Crimea under the disguise of an ongoing surprise inspection taking place in the western and central military districts.[42] The possibility that Russia might be preparing the ground for a military invasion under the cover of military exercises apparently worries Minsk as well.

Therefore, Belarus is trying to make the exercise as transparent for the West as possible, thus increase the political costs of a potential aggression for Russia.[43] Minsk published the exact extent of the exercise that is going to take place on

38   BOHDAN, S. "The West-2017 Belarus-Russian Military Exercise: Smaller Than Anticipated". Belarus Digest. March 24., 2017 – http://belarusdigest.com/story/west-2017-belarus-russian-military-exercise-smaller-anticipated-29513_ Accessed on June 27., 2017.

39   "Dalia Grybauskaitè: 'West-2017' military drill worrying." Belsat. February 10., 2017 – http://belsat.eu/en/news/dalya-grybauskajtse-vuchenni-zahad-2017-chakaem-z-nepakoem/ Accessed on June 27., 2017.

40   KOWALIK, T. K.; JANKOWSKI, D. P. "The dangerous tool of Russian military exercises." Center for European Policy Analysis. May 9., 2017 – http://cepa.org/EuropesEdge/The-dangerous-tool-of-Russian-military-exercises Accessed on June 27., 2017.

41   The Russian MoD clarified that the number of 4,000 railway wagons is actually only 2,000 as the tender calls for „round trip" transportation. Also, the ministry disclosed information on the quantity of wagons used during previous exercises, a number higher in all two cases than in the case of the upcoming exercise (6,000 in 2009 and 2,500 in 2013 respectively). BOHDAN, S. "The West-2017 Belarus-Russian Military Exercise."

42   Forty Il–76 military transport aircraft were observed departing the exercise area, and were later observed in Crimea. DUGAS, M. E. Between Georgia and Crimea: The Social Dimensions of War for the Russian Military. Wellesley: Wellesley College. April, 2016 – http://repository.wellesley.edu/cgi/viewcontent.cgi?article=1432&context=thesiscollection Accessed on June 27., 2017; p. 66.

43   KOWALIK–JANKOWSKI "The dangerous tool of Russian military exercises."

Belarusian territory. Approximately 3000 Russian military personnel and some 280 vehicles are going to exercise on Belarusian territory. This is significantly smaller than the preceding Zapad 2009 exercise was,[44] and is indeed not enough for occupying Belarus – unless significant reinforcements are sent in under whatever pretext.

Hence, Minsk also invites approximately 80 external observers as well to increase transparency of the whole Zapad 2017.[45] This is done in order to ensure the protection of Belarus against Russian informational measures and military operations based on them. For example, the presence of objective, international observes during the exercise would make it a lot harder for Russia to make groundless claims and use them to justify a military aggression.

THE THEORY AT WORK: THE ANNEXATION OF THE CRIMEA AND THE OPERATION IN EASTERN UKRAINE

The role of non-military measures

The increased importance the theorists had attributed to the non-military measures was well reflected in practice during the Ukraine war. As it was presented earlier, some elements of hybrid war are already being employed in a period when the diverging interests of the parties have not yet rose to the level of open conflict of interests. This means that the measures used in this preparatory phase will likely remain below the level of perception. Also, as they "do not differ that much from the traditional diplomatic and soft coercion activities of Russia"[46] it is even harder to tell if what we perceive is part of an already ongoing hybrid operation or it is just regular Russian diplomacy in action. Thus, it is also very problematic to determine when the hybrid war against Ukraine has been launched. There are allegations that the creation of an extensive intelligence network and support base in the Crimea has already started after the 2004 Orange Revolution.[47] So Russia at least started to map out the possible weaknesses to be exploited in case of a future annexation ten years before it had actually taken place.

---

44   BOHDAN. "The West-2017 Belarus-Russian Military Exercise."
45   "Belarus to invite over 80 international observers for Zapad 2017 army exercise." Belarus News, July 17., 2017 – http://eng.belta.by/society/view/belarus-to-invite-over-80-international-observers-for-zapad-2017-army-exercise-103395-2017/ Accessed on June 27., 2017.
46   RÁCZ "Russia's Hybrid War in Ukraine." p. 58.
47   DUGAS "Between Georgia and Crimea." p. 78.

As soon as Yanukovich was toppled and fled from Kiev the events speeded up and full-blown information war was launched targeting the Russian ethnic population by presenting fake news on the "Kiev junta" attacking Russian minorities on a mass scale. In the meantime, Russian intelligence services mimicked the revolutionary process of Maidan and presented mass protests as if they were an organic resistance of the population while in reality they were well orchestrated actions.[48]

Another major tool Moscow extensively used in Crimea and Eastern Ukraine was a number of proxy actors ranging, from ex-members of Russian spetsnaz and security services to Kuban Cossacks, criminal networks and even Serbian Chetniks,[49] whose role was to occupy administrative buildings, establish control over main roads and airports and to organize armed resistance. Their operations were coordinated by GRU operatives on the ground, while the operationally more advanced tasks were carried out by actual Russian military forces without insignia.[50] The little green men – or the polite riflemen (vezhliviye avtomatchiki) as the Russian propaganda referred to them – occupied the airports of Simferopol and Sevastopol and the parliament in Simferopol on February 27-28.[51] In the meantime, the state television, air defense bases and command posts were occupied. Moscow was keen on to avoid casualties on both sides, therefore military bases with lesser importance were only surrounded by the Russian Special Forces, who waited until the encircled, demoralized Ukrainians surrendered.[52]

Military measures
As Chekinov and Bogdanov put it, the role of conventional military measures in hybrid warfare is often restricted to the final phase of operation, when the achieved goals are to be consolidated through the deployment of military force. In the case of Crimea the first Russian motorized rifle brigade set foot

---

48   Ibid. p. 128
49   "Little Green Men": a primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014. U.S. Army Special Operations Command. June, 2015 – www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf   Accessed on July 7., 2017; p. 44.
50   BARTLES, C. K.; MCDERMOTT, R. N. "Russia's Military Operation in Crimea. Road-Testing Rapid Reaction Capabilities." Problems of Post-Communism. November/December, 2014 p. 57. It is important to remind here to that special operations are not regarded as military measures in the relevant Russian literature describing hybrid war.
51   WILSON, A.: Ukraine Crisis: What it Means for the West. New Haven: Yale University Press. 2014; p. 111.
52   BARTLES, MCDERMOTT. "Russia's Military Operation in Crimea."

on Ukrainian territory only on March 12.[53] The foremost aim of the deployed conventional forces was to secure the occupied territory from interventions both from land and sea. Accordingly, Russia has deployed Bastion P anti-ship missile complexes to Sevastopol, air-defense forces,[54] artillery and Grad multiple rocket launchers to the Northern border of Crimea.[55]

Despite the success in Crimea, Russia could not employ its hybrid strategy with the same effectiveness in Eastern Ukraine. In contrast to the Crimea operation, Moscow had to rely heavily on its conventional military assets. It was largely due to two factors. First, by this time the Ukrainian forces had managed to achieve a higher readiness, and second, there was a clear political will to counter the Russian intervention. While threat by the Russian conventional forces in the form of a large-scale military exercise[56] had worked during the occupation of Crimea, it fell short in Eastern Ukraine as Kiev had realized by then that the Kremlin was not willing to pay the price for an open full-scale aggression against Ukraine. As a result, Moscow found itself in a dilemma to either let the cover of its – not really credible –covert intervention fully blown or to sacrifice the territory it had already gained. The Kremlin chose the first option, which led to large scale conventional military intervention among other cases in Ilovaysk in August 2014 and in Debaltsevo early 2015.

THE SYRIA OPERATION: WHAT CAN IT TELL US ABOUT THE CAPABILITIES OF THE RUSSIAN MILITARY

After years of technical and advisory assistance to the Assad regime, Moscow deployed military forces to Syria in September 2015 to tip the balance of the ongoing war in favor of its protégé. While the declared aim of Moscow's intervention was to destroy the ISIS, the targets bombed by the Russian

---

53   DUGAS. Between Georgia and Crimea.p.69.
54   Ibid.
55   BUGRIY, M. "The Crimean Operation: Russian Force and Tactics." The Jamestown Foundation. April 1, 2014 – https://jamestown.org/program/the-crimean-operation-russian-force-and-tactics/ Accessed on July 7., 2017.
56   By the end of March a 40–50 thousand strong force advanced to the Ukrainian border as part of a snap exercise. WILSON, A. Ukraine Crisis: What it Means for the West. p. 129.

Aerospace Forces proved already in the very beginning of the intervention that this was merely a secondary objective.[57]

The capability to project power in remote areas

The intervention in Syria was the first expeditionary mission of Moscow beyond the so-called near abroad since the war in Afghanistan. While the mission according to Russian sources was planned for a period of 3-4 months[58] the Russian engagement in Syria is still going on as of the writing of this paper, even though Vladimir Putin has announced the withdrawal in March 2016.[59] It is unknown exactly when the decision was taken on the force deployment, but it is believed that concrete military preparation did not start before the summer of 2015.[60] It means that in a couple of months Moscow managed to deploy a relatively capable force consisting of at least 71 fixed-wing aircraft,[61] an unknown number of helicopters, as well as other vehicles. Even more surprisingly for Western military observers, the Russian Aerospace Forces were able to sustain a very high number of daily sorties[62] often larger than the number conducted by the U.S. led coalition forces in a whole month.[63] When in April 2017 it was announced that Russia has withdrawn almost half of its

---

57   ",More than 90%' of Russian airstrikes in Syria have not targeted Isis, US says." The Guardian. October 7., 2015 – https://www.theguardian.com/world/2015/oct/07/russia-airstrikes-syria-not-targetting-isis Accessed on July 8., 2017.

58   "Russian air strikes in Syria to last 3–4 months – Putin ally." Reuters. October 2., 2015 – http://in.reuters.com/article/mideast-crisis-russia-strike-idINKCN0RW0I220151002 Accessed on July 8., 2017.

59   "9,000 sorties, 400 localities freed: What Russia has achieved during its 5-month Syria operation." RT. March 14., 2016 – https://www.rt.com/news/335596-russia-syria-operation-results/ Accessed on July 8., 2017.

60   BASSAM, L.; PERRY T. "How Iranian general plotted out Syrian assault in Moscow." Reuters. October 6., 2015 – https://www.reuters.com/article/us-mideast-crisis-syria-soleimani-insigh-idUSKCN0S02BV20151006 Accessed on July 8., 2017.

61   Moscow has deployed 34 fixed-wing aircraft in the first stage of the mission supplementing them with additional 37 after mid-November 2015. MARCUS J. "Syria: What can Russia's military do?" BBC. October 7., 2015 – http://www.bbc.com/news/world-asia-34411477 Accessed on July 8., 2017. GORENBURG, D. "What Russia's Military Operation in Syria Can Tell Us About Advances in its Capabilities." PONARS Eurasia March, 2016 – http://www.ponarseurasia.org/memo/advances-russian-military-operation Accessed on July 8., 2017; p. 1.

62   The number of sorties reached 189 on 24. December, 2015. GORENBURG. "What Russia's Military Operation in Syria Can Tell Us About Advances in its Capabilities."

63   SENGUPTA, K. "War in Syria: Russia's ,rustbucket' military delivers a hi-tech shock to West and Israel." The Independent. January 29., 2016 – http://www.independent.co.uk/news/world/middle-east/war-in-syria-russia-s-rustbucket-military-delivers-a-hi-tech-shock-to-west-and-israel-a6842711.html Accessed on July 8., 2017.

---

aviation group stationed on the Hmeymim airbase, the overall figure of sorties over Syria stood at more than 23,000.[64]

Russia has a state-of-the-art military – and it wants you to know that

Another remarkable feature of the Russian intervention was the wide range of tools Moscow has employed. On the one hand, Syria has provided a test field for the new weapons and technologies, on the other hand, the Kremlin made sure to widely publicize their use as well. During the operation the Russian military showed the effective employment of capabilities that the outside world had not realized that Russia possessed. Among those were the Kalibr cruise missiles which were launched multiple times from corvettes and frigates stationed in the Caspian and a submarine from the Mediterranean Sea.[65] Russian air defense capabilities apparently were also found as worrisome features of Russia's renewed military, as well as its electronic jamming systems like the Krasuha 4.[66] The only deficiency in Russian capabilities visible to the outside world was the less than glorious performance of the country's sole aircraft carrier, the Kuznetsov's,[67] which otherwise did not play a significant role in the mission. The newly established Russian tier one special force, the KSO's Syrian presence was widely broadcast in Russian media, and from the footage it turned out that their equipment closely resembled those used by their Western counterparts,[68] testifying to the distinctive role Russia attributes to the special operations. While Russia showed to the world that it owns high-tech precision weapons, their mere roughly 20% ratio[69] as compared to the overall number of bombs dropped over Syria likely suggests that Russia has a limited stockpile at its disposal.

---

64   "Russia has withdrawn almost half of its aviation group based on Hmeymim airbase in Syria." Ministry of Defence of the Russian Federation. April 26., 2017 – http://eng.mil.ru/en/news_page/country/more.htm?id=12120736@egNews Accessed on July 8., 2017.

65   GORENBURG. "What Russia's Military Operation in Syria Can Tell Us About Advances in its Capabilities."

66   SENGUPTA. "War in Syria."

67   FILIPOV, D.; ROTH, A. "Russian jets keep crashing, and it may be an aircraft carrier's fault." The Washington Post. December 5, 2016 – https://www.washingtonpost.com/world/russia-just-lost-its-second-warplane-in-a-month-of-syria/2016/12/05/f8353be8-bad8-11e6-817f-e3b588251d1e_story.html?utm_term=.859b1e165e16 Accessed on July 8., 2017.

68   GIBBONS-NEFF, T. "New battlefield video shows how Russia's elite KSO military unit is fighting in Syria." The Washington Post. December 13., 2016 – https://www.washingtonpost.com/news/checkpoint/wp/2016/12/13/new-battlefield-video-shows-how-russias-elite-kso-military-unit-is-fighting-in-syria/?utm_term=.a0243a3633ca Accessed on July 8., 2017 .

69   GORENBURG. "What Russia's Military Operation in Syria Can Tell Us About Advances in its Capabilities."

Privatization of violence

As it was already mentioned in relation to the war in Ukraine, the Kremlin tends to rely more and more on proxy actors to outsource military tasks. Moscow has two main reasons doing so. First, Moscow uses them for the purpose to disguise Russian military presence in conflicts in which Russia is officially not involved. Second, the Kremlin is hesitant to pay the political price for losing soldiers on the ground in higher numbers. Consequently, these so-called proxy actors are generally tasked with the riskiest missions.[70] An increasingly significant constituent of these proxies is the mercenary company Wagner Group, that has already been present in Ukraine[71] and is now taking a major role in fights in Syria. Unlike its Western counterparts that generally are contract partners of the respective ministries, and are taking roles in personnel and site protection, Wagner's activities – which, according to the law are illegal in Russia[72] – are well beyond providing a service upon contract. Wagner's training camp is in Molkino, the same village where the GRU's 10th special service brigade's training site is located.[73] Moreover, Wagner mercenaries in Syria use weapons issued only to GRU special forces units.[74] The company's close relationship with Russian military intelligence is also shown by the fact that its founder, Dmitry Utkin was an officer of the 2nd Spetsnaz Brigade until 2013.[75] Wagner is believed to be under the control of FSB and GRU officers in Syria[76] and took part in both the first and the second

---

70   Moreover, some of the proxies are deliberately tasked with potentially deadly missions. A Russian expert during a conversation with one of the authors referred to talks with a local FSB officer who stated that his agency encourages so called „useful idiots" to fight in Ukraine. Allegedly the officer freely discussed that these persons – based on their radical political views – represent a security problem for Russia and the FSB sends them to Ukraine with the hope that they would not return.

71   Wagner was involved in the battle for Debaltseve in January 2015, for instance. QUINN, A. "Vladimir Putin sent Russian mercenaries to ‚fight in Syria and Ukraine.'" The Telegraph. March 30., 2016 – http://www.telegraph.co.uk/news/2016/03/30/vladimir-putin-sent-russian-mercenaries-to-fight-in-syria-and-uk/ Accessed on July 8., 2017.

72   "More Russian Fighters from Private 'Wagner Group' Die in Syria." The Moscow Times. July 9., 2017 – https://themoscowtimes.com/news/more-undocumented-russian-fighters-from-private-wagner-group-die-in-syria-57499 Accessed on July 8., 2017.

73   QUINN. "Vladimir Putin sent Russian mercenaries to ‚fight in Syria and Ukraine'."

74   GOSTEV, A.; COALSON, R. "Russia's Paramilitary Mercenaries Emerge From The Shadows." Radio Free Europe/Radio Liberty. December 16, 2016 – https://www.rferl.org/a/russia-paramilitary-mercenaries-emerge-from-the-shadows-syria-ukraine/28180321.html Accessed on July 8., 2017.

75   GALEOTTI, M. "Moscow's Mercenaries in Syria." War on the Rocks. April 5., 2016 – https://warontherocks.com/2016/04/moscows-mercenaries-in-syria/ Accessed on July 9., 2017.

76   "Vagner poteryal ispolnyatelya." [Wagner lost its operative] RBK. March 6., 2017 – http://www.rbc.ru/newspaper/2017/03/07/58bd3bc49a7947df4da2e17a Accessed on July 9., 2017.

Palmyra offensives.[77] Based on interviews with ex-members of the groups the company does not only provide infantrymen but also has air defense, heavy artillery and tanks in Syria.[78] It is unknown exactly what casualties the group has suffered in Syria, but according to an article published in August 2016, the figure was approximately 500-600.[79] It is in striking contrast to the official military losses of 30 soldiers.[80] Besides Wagner, Moscow has recently sent an estimated number of 800 Chechen and Ingush soldiers to Syria, which suggests that despite the decreasing official military presence, Moscow's intervention is far from over.

Russia's intervention in Syria uncovered military capabilities not known to the outside world before. While Moscow's decision to intervene was probably forced by the dramatically changing situation on the ground in favor of the opposition, it would be a mistake to think of it as a unique case. Russia's emerging assertive foreign policy suggests that other expeditionary missions are to be expected in areas of significant interest to Moscow. In a recent article Gerasimov emphasized the necessity to study the "problems of organizing and carrying out regrouping of forces to remote theater[s]."[81] Consequently, a similar scenario is at least in the mind of the Russian military leadership.

Conclusions

Valeriy Gerasimov's famous article published in 2013 has not constituted a fundamental change in Russian military thinking. If it was revolutionary, it was only so to unaware Western observers. If fact, the article of the Chief of the Russian General Staff was the result of a long, gradual evolutionary process of Russian military thinking about the nature of war.

---

77   LEVIEV, R. "They fought for Palmyra… again: Russian mercenaries killed in battle with ISIS." Conflict Intelligence Team. March 22., 2017 – https://citeam.org/they-fought-for-palmyra-again-russian-mercenaries-killed-in-battle-with-isis/ Accessed on July 9., 2017.

78   Ibid. and GALEOTTI. "Moscow's Mercenaries in Syria."

79   SPARKS, J. "Revealed: Russia's ‚Secret Syria Mercenaries.'" Sky News. August 10., 2016 – http://news.sky.com/story/revealed-russias-secret-syria-mercenaries-10529248   Accessed on July 09., 2017.

80   HAUER, N. "Putin Has a New Secret Weapon in Syria: Chechens." Foreign Policy. May 4., 2017 – http://foreignpolicy.com/2017/05/04/putin-has-a-new-secret-weapon-in-syria-chechens/?utm_content=buffer03686&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer Accessed on July 8., 2017.

81   GERASIMOV. "Mir na granyah voyni."

This process has not stopped since 2013 either. Russian military thinkers keep studying the present armed conflicts, including the ones Russia is engaged in, and are factoring in the lessons learned into their concepts. Close attention is paid to military technological developments and to the ways they shape wars and warfighting. Hence, contemporary Russian military thinking is preparing for an increasingly network-centric, high-precision, mostly contactless war. In such a war, non-military components, such as informational, cyber, special operations and economic tools and means, together with the protest potential of the local population play a key, often decisive role. Meanwhile, conventional military engagement takes place only in the later phases of the conflicts. Russia's strategic military exercises clearly reflect these assumptions.

Experience gained from Ukraine and Syria also shape the Russian thinking about the conflicts of the 21st century. In Ukraine the annexation of the Crimea was a masterful realization of how Gerasimov described "new generation warfare." However, in Eastern Ukraine a similar start led to a fundamentally different outcome. It would be a mistake to assume that Russia has not done its best to analyze the reasons of the Donbas failure, even though it can hardly be done publicly, because it would mean admitting Russia's participation in the conflict.

Meanwhile, in Syria Russia managed to conduct its first-ever expeditionary, combined arms operation. Several new, or refurbished, modernized capabilities have been tested, such as carrier-based air operations as well as high-precision, long-range missile strikes. Moreover, Syria was the debut of another new phenomenon, namely the emergence of private military contractors, namely the Wagner Group alongside the regular Russian army. Syria clearly demonstrated that expeditionary operations, even if of limited size, have become integral parts of the Russian military inventory.

All these development processes deserve continuous, close – and well-resourced – attention from the side of NATO, Hungary included. The strategic surprise Russia was able to impose on the West by the swift, though illegal annexation of the Crimea must not get repeated.

Krisztián Jójárt completed his M.A. in Security and Defense Policy at the National University of Public Service in 2013, and is currently a post-graduate student of international relations at the Corvinus University in Budapest. His most recent article analyzes Belarusian-Russian military relations

and was published in the 2016/2 issue of the journal Nemzet és Biztonság (Nation and Security) in Hungarian. He can be reached at: jojart.krisztian@gmail.com.

ANDRÁS RÁCZ Ph.D is Associate Professor of the Pázmány Péter Catholic University in Budapest, Hungary. Besides, he works as Senior Research Fellow at the Centre for Strategic and Defense Studies of the National University of Public Service. Between 2014 and 2016 he worked as Senior Research Fellow at the Finnish Institute of International Affairs (FIIA) in Helsinki. A specialist of Russian and post-Soviet security policy, he defended his PhD in Modern History at the Eötvös Loránd University in Budapest in 2008. He was a member of the European Foreign and Security Policy Studies Programme (EFSPS) of the Volkswagen Foundation, and was Visiting Fellow at the Transatlantic Academy of the German Marshall Fund in Washington D.C. in 2011-2012. His last monograph was published in 2015 in Helsinki, and is titled: "Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist." He can be reached at: andras.racz@gmail.com.

BIBLIOGRAPHY

"*9,000 sorties, 400 localities freed: What Russia has achieved during its 5-month Syria operation.*" RT. March 14., 2016 – https://www.rt.com/news/335596-russia-syria-operation-results/ Accessed on July 8., 2017.

BARTLES, C. K. "*Getting Gerasimov Right*" in Military Review. January-February, 2016 – http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf Accessed on June 28., 2017.

BARTLES, C. K.; MCDERMOTT, R. N. "*Russia's Military Operation in Crimea. Road-Testing Rapid Reaction Capabilities.*" Problems of Post-Communism. November/December, 2014.

BARVINENKO, V. "*Ot asteroida i provokatora*" [From asteroid and provocateur] in Voyenno-Promishlenniy Kurer. June 7., 2017 – http://www.vpk-news.ru/articles/37129 Accessed on June 27., 2017.

BASSAM, L.; PERRY T. "*How Iranian general plotted out Syrian assault in Moscow.*" Reuters. October 6., 2015 – https://www.reuters.com/article/us-mideast-crisis-syria-soleimani-insigh-idUSKCN0S02BV20151006 Accessed on July 8., 2017.

"*Belarus to invite over 80 international observers for Zapad 2017 army exercise.*" Belarus News, July 17., 2017 – http://eng.belta.by/society/view/belarus-to-invite-over-80-international-observers-for-zapad-2017-army-exercise-103395-2017/ Accessed on June 27., 2017.

BOHDAN, S. "*The West-2017 Belarus-Russian Military Exercise: Smaller Than Anticipated*". Belarus Digest. March 24., 2017 – http://belarusdigest.com/story/west-2017-belarus-russian-military-exercise-smaller-anticipated-29513 Accessed on June 27., 2017.

BUGRIY, M. "*The Crimean Operation: Russian Force and Tactics.*" The Jamestown Foundation. April 1., 2014 – https://jamestown.org/program/the-crimean-operation-russian-force-and-tactics/ Accessed on July 7., 2017.

CHEKINOV, S. – BOGDANOV S. "The Nature and Content of a New-Generation War." Military Thought, October-December 2013 – http://www.eastviewpress.com/Files/ MT_FROM%20THE%20 CURRENT%20ISSUE_No.4_2013.pdf Accessed on June 27., 2017.

COALSON, R. *Twitter post.* Twitter. June 21., 2014 – https://twitter.com/coalsonr/status/480374222997692416 Accessed on June 27., 2017.

"*Dalia Grybauskaitė: 'West-2017' military drill worrying.*" Belsat. February 10., 2017 – http://belsat.eu/en/news/dalya-grybauskajtse-vuchenni-zahad-2017-chakaem-z-nepakoem/ Accessed on June 27., 2017.

DUGAS, M. E. *Between Georgia and Crimea: The Social Dimensions of War for the Russian Military.* Wellesley: Wellesley College. April, 2016 – http://repository.wellesley.edu/cgi/viewcontent.cgi?article=1432&context=thesiscollection Accessed on June 27., 2017.

FILIPOV, D.; ROTH, A. "*Russian jets keep crashing, and it may be an aircraft carrier's fault.*" The Washington Post. December 5., 2016 – https://www.washingtonpost.com/world/russia-just-lost-its-second-warplane-in-a-month-of-syria/2016/12/05/f8353be8-bad8-11e6-817f-e3b588251d1e_story.html?utm_term=.859b1e165e16 Accessed on July 8., 2017.

GALEOTTI, M. "*It's the Russians Wot Done It.*" The Moscow Times. June 20., 2017 – https://themoscowtimes.com/articles/its-the-russians-wot-done-it-58228 Accessed on June 27., 2017.

GALEOTTI, M. "*Moscow's Mercenaries in Syria.*" War on the Rocks. April 5., 2016 – https://warontherocks.com/2016/04/moscows-mercenaries-in-syria/ Accessed on July 9., 2017.

GALEOTTI, M. "*The 'Gerasimov Doctrine' and Russian Non-Linear War.*" In Moscow's Shadows [blog] July 6., 2014 – https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ Accessed on June 27., 2017.

GAREEV, M. *If War Comes Tomorrow? The Contours of Future Armed Conflict.* Translated by Yakov Vladimirovich Fomenko. Abingdon: Routledge, 1998.

GERASIMOV, V. "*Mir na granyah voyni. Malo uchitivat' sevodniashnee vizovi, nado prognozirovat' budushchie.*" [Peace on the brink of war. Not enough to calculate with challenges of the present, should predict future ones] Voyenno-Promishlenniy Kurer. March 15., 2017 – http://www.vpk-news.ru/articles/35591 Accessed on July 3., 2017.

GERASIMOV, V. "*Tsennosti nauki v predvidenii*" [The Value of Science in Prediction] Voyenno-Promishlenniy Kurer. February 27., 2013 – http://www.vpk-news.ru/articles/14632 Accessed on June 27., 2017.

GIBBONS-NEFF, T. "*New battlefield video shows how Russia's elite KSO military unit is fighting in Syria.*" The Washington Post. December 13., 2016 – https://www.washingtonpost.com/news/checkpoint/wp/2016/12/13/new-battlefield-video-shows-how-russias-elite-kso-military-unit-is-fighting-in-syria/?utm_term=.a0243a3633ca Accessed on July 8., 2017.

GORENBURG, D. "*What Russia's Military Operation in Syria Can Tell Us About Advances in its Capabilities.*" PONARS Eurasia March, 2016 – http://www.ponarseurasia.org/memo/advances-russian-military-operation Accessed on July 8., 2017.

GOSTEV, A.; COALSON, R. "*Russia's Paramilitary Mercenaries Emerge From The Shadows.*" Radio Free Europe/Radio Liberty. December 16., 2016 – https://www.rferl.org/a/russia-paramilitary-mercenaries-emerge-from-the-shadows-syria-ukraine/28180321.html Accessed on July 8., 2017.

HAUER, N. "*Putin Has a New Secret Weapon in Syria: Chechens.*" Foreign Policy. May 4., 2017 – http://foreignpolicy.com/2017/05/04/putin-has-a-new-secret-weapon-in-syria-chechens/?utm_content=buffer03686&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer Accessed on July 8., 2017.

KISELYEV, V. A: "*K kakim voynam neobhodimo gotovit' Vooruzhennie Sili Rossii.*" [What Types of Wars must the Russian Armed Forces be Have to Prepared for] in Voyennaya Misl No. 3/2017.

KOWALIK, T. K.; JANKOWSKI, D. P. "*The dangerous tool of Russian military exercises.*" Center for European Policy Analysis. May 9., 2017 – http://cepa.org/EuropesEdge/The-dangerous-tool-of-Russian-military-exercises Accessed on June 27., 2017.

LAMBETH, B. S. "*Russia's Wounded Military.*" Foreign Affairs. March/April, 1995.

LEVIEV, R. "*They fought for Palmyra... again: Russian mercenaries killed in battle with ISIS.*" Conflict Intelligence Team. March 22., 2017 – https://citeam.org/they-fought-for-palmyra-again-russian-mercenaries-killed-in-battle-with-isis/ Accessed on July 9., 2017.

"Little Green Men": a primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014 U.S. Army Special Operations Command. June, 2015 – www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf Accessed on July 7., 2017.

MARCUS J. "*Syria: What can Russia's military do?*" BBC. October 7., 2015 – http://www.bbc.com/news/world-asia-34411477 Accessed on July 8., 2017.

MATTSON, P. "*Russian operational art in the fifth period: Nordic and Arctic applications.*" Revista de Ciências Militares, Vol. 1, N.º 1, May 2013; p. 29–47. – http://www.iesm.pt/cisdi/revista/Artigos/Revista_1_Artigo_1.pdf. Accessed on June 27., 2017.

McDERMOTT, R. N. "*Learning From Today's Wars. Does Russia Have a Gerasimov Doctrine?" in Parameters.* Spring, 2016 – https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2016/12_McDermott.pdf Accessed on June 27., 2017.

"*More Russian Fighters from Private 'Wagner Group' Die in Syria.*" The Moscow Times. July 9., 2017 – https://themoscowtimes.com/news/more-undocumented-russian-fighters-from-private-wagner-group-die-in-syria-57499 Accessed on July 8., 2017.

"*More than 90%' of Russian airstrikes in Syria have not targeted Isis, US says.*" The Guardian. October 7., 2015 – https://www.theguardian.com/world/2015/oct/07/russia-airstrikes-syria-not-targetting-isis Accessed on July 8., 2017.

NORBERG, J. *Training to Fight - Russia's Major Military Exercises 2011–2014;* Stockholm: FOI. December, 2015. – https://www.foi.se/report-search/pdf?

fileName=D:%5CReportSearch%5CFiles%5C8e2dc822-a31c-4f6c-aecd-954375e3fe31.pdf Accessed on June 26., 2017.

PERSHUTKIN, S. *"Talanti – v kurszanti. Dla oruzhia na novih fizicheskih printsipah nuzhni offitseri-intellektuali i sovietskie metodiki."* [The talented – to the military academy. For the weapons based on new physical principles intellectual officers and soviet methodos are needed] in Voyenno-Promishlenniy Kurer. June 14., 2017 – http://www.vpk-news.ru/articles/37230 Accessed on June 27., 2017.

QUINN, A. *"Vladimir Putin sent Russian mercenaries to 'fight in Syria and Ukraine'."* The Telegraph. March 30., 2016 – http://www.telegraph.co.uk/news/2016/03/30/vladimir-putin-sent-russian-mercenaries-to-fight-in-syria-and-uk/ Accessed on July 8., 2017.

RÁCZ, A. *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist.* Helsinki: The Finnish Institute of International Affairs. June 16., 2015 – http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine/ Accessed on June 27., 2017; p. 36.

"Russia has withdrawn almost half of its aviation group based on Hmeymim airbase in Syria." Ministry of Defence of the Russian Federation. April 26, 2017 – http://eng.mil.ru/en/news_page/country/more.htm?id=12120736@egNews Accessed on July 8., 2017.

"Russian air strikes in Syria to last 3–4 months – Putin ally." Reuters. October 2., 2015 – http://in.reuters.com/article/mideast-crisis-russia-strike-idINKCN0RW0I220151002 Accessed on July 8., 2017.

SENGUPTA, K. *"War in Syria: Russia's 'rustbucket' military delivers a hi-tech shock to West and Israel."* The Independent. January 29., 2016 – http://www.independent.co.uk/news/world/middle-east/war-in-syria-russia-s-rustbucket-military-delivers-a-hi-tech-shock-to-west-and-israel-a6842711.html Accessed on July 8., 2017.

SPARKS, J. *"Revealed: Russia's 'Secret Syria Mercenaries'."* Sky News. August 10., 2016 – http://news.sky.com/story/revealed-russias-secret-syria-mercenaries-10529248 Accessed on July 09., 2017.

THOMAS, T. *Thinking Like a Russian Officer. Basic Factors and Contemporary Thinking on the Nature of War.* Fort Leavenworth: Foreign Military Studies Office. April 2016.

"Vagner poteryal ispolnyatelya" [Wagner lost its operative] RBK. March 6., 2017 – http://www.rbc.ru/newspaper/2017/03/07/58bd3bc49a7947df4da2e17a   Accessed on July 9., 2017.

VASILYEV, S. – KRIVORUCHKO, V. *"Nash nevniatniy otvet agressoru – chast' I."* [Our inarticulate response to the aggressor – part one] in Voyenno-Promishlenniy Kurer. May 17., 2017 – http://www.vpk-news.ru/articles/36744 Accessed on June 27., 2017.

VASILYEV, S. – KRIVORUCHKO, V. *"Nash nevniatniy otvet agressoru – chast' II."* [Our inarticulate response to the aggressor – part two] in Voyenno-Promishlenniy Kurer. May 24., 2017 – http://www.vpk-news.ru/articles/36878 Accessed on June 27., 2017.

WILSON, A. *Ukraine Crisis: What it Means for the West.* New Haven: Yale University Press. 2014.

PETER A. KISS
Meeting the Gray Zone Challenge

ABSTRACT: The generally accepted Western model of peace and armed conflict (peace – declaration of war – large-scale military operations – armistice – peace treaty) is a rare exception. Competing states and non-state actors far more frequently assert their interest in the intermediate, ambiguous social and political space between peace and war – the gray zone. Emerging powers and powerful non-state actors are challenging the current international order in this intermediate space, and are doing so with some success. Unless the Western nations recognize the gray zone as a legitimate space for conflict and competition, and find ways to strengthen the societal pillar of their defensive structures, they shall have two alternatives: tolerate these gray zone challenges, or escalate them into the very dark gray or black part of the spectrum – to war.

THE BLACK, THE WHITE AND THE GRAY

Our usual understanding of war and peace proceeds from certain assumptions. First of all, it is the affair of nation states or alliances, non-state actors play no role in it at all. Second, it is an either-or proposition: nations are either at peace with each other, or they are at war, and the transition from peace to war is symbolized by a declaration of war, the one from war to peace by a peace treaty (or outright annexation). Third, one set of laws applies when a nation is at peace, and another when it is at war. We have well-developed mental models and terminology to conceptualize and describe both peace and war, and even better developed doctrines to conduct them.

However, the real world hardly ever works this way. The orderly procession from peace through declaration of war, large-scale military operations and armistice to a return to peace again is the rare exception, rather than the

rule. In reality there is an intermediate, ambiguous social and political space between white (peace) and black (war), where competing states and non-state actors can assert their interest by using some force, but without reaching any recognized threshold of international war.[1] This gray zone between peace and war can be quite narrow and restricted, as it was during the cold war, for example, or quite extensive, as it is today. (fig 1.)
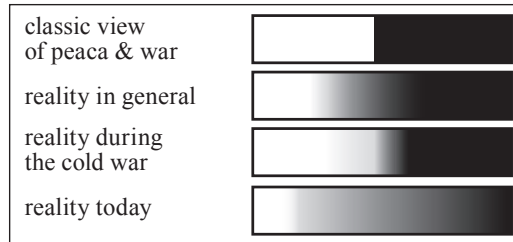
Figure 1.
The gray social and political space between peace and war[2]

One of America's most colorful Generals, George S. Patton said at one time, that „no one is thinking if everyone is thinking alike."[3] General Patton may have been a controversial figure, but this one-liner of his could serve as the motto of this conference, because it neatly sums up the drivers of the security challenges of the 21st century. In a good part, due to "thinking alike" we have become victims of our own success. The economic, political and military power of the western nations (and I include in this category such non-western nations as New Zealand, Singapore, Israel, and even India) has created a stable world order that has ensured reasonable peace and growing prosperity for its participants. At the same time, their military power has practically guaranteed defeat for those who would openly challenge this world order. This has worked for several decades, but today this status quo is under considerable strain.

---

1   In the 100 years between 1915 and 2015 the United States was involved in seven international conflicts, but deployed its armed forces on nealy 60 occasions to advance its interests by force of arms. The Gray Zone. Tampa: US Special Operations Command, 2015.
2   KISS, Peter A. Hybrid Warfare and Conflict in the Gray Zone. Lecture at the Staff Officers' Military Terminology Course, Budapest, 2016.
3   WILLIAMSON, Porter B. General Patton's Principles for Life and Leadership. Tucson: Management & Systems Consultants. p. 151.

CHALLENGES IN THE GRAY ZONE

Increasingly powerful non-state actors with an international agenda, emerging regional powers that aspire to expand their sphere of influence, as well as countries that strive to reclaim their former level of influence either question, or reject outright, the legitimacy of the norms, principles and rules of this international order, and seek to change it. However, the modern world's political, economic and social interdependence has made the cost of major aggressive action so high that alternative ways must be found to engineer significant revisions of the status quo.[4] By not "thinking alike," and relying on such technological advances as cyber weapons, social media, and cheap, instant, worldwide communications tools, both states and non-state actors are finding alternatives. They are achieving warlike objectives without stepping over a recognizable threshold that would engender a powerful military response. Their methods are as diverse as are their goals, and as the theaters where the conflicts take place.

a. By creating artificial islands in the South China Sea, and asserting its sovereignty over them, China is expanding its maritime territory (and is acquiring potentially rich natural resources) at the expense of its neighbors. By saturating the contested areas with its fishing fleet, it puts the onus of responsibility, for any civilian casualties and loss of civilian vessels, as well as the risk of causing a casus belli on the nations on whose territory it is encroaching.

b. Russia is perceived as a major threat to the security of the Baltic countries (and by extension to NATO), not only because of its large conventional forces and nuclear weapons, but also due to its ability to mobilize the sizeable Russian populations in those states against their own government. In the rebellious eastern provinces of Ukraine and in the annexation of the Crimea Russia has already demonstrated its ability to advance its interests by carefully calibrated violence, but without risking international war.

c. Although the Islamic State has overreached itself and faces defeat in Iraq and very likely in Syria, its ideological influence has expanded throughout the MENA region, as well as into Sub-Saharan Africa and is creeping into Europe.

---

4   MICHAEL J. Mazarr. Mastering the Gray Zone: Understanding a Changing Era of Conflict. Carlisle Barracks: US Army War College Press, 2015.

137

d. North Korea has been probing the limits of its neighbors' (and the United States') patience and tolerance with occasional small scale attacks, and has managed to change the power balance of the Northeast Asia region.[5]

e. Israel has had no problems defeating the regular armed forces of its neighbors, but so far it has had grave difficulties in coming to grips with its two non-state adversaries, Hezbollah and Hamas.

f. Through mobilization of Jammu and Kashmir's Muslim population, fomenting terrorism within India, and occasionally delivering short, sharp, but limited ground attacks with conventional forces, Pakistan has prevented the full integration of the state into India for several decades.

g. The adherents of the radical and violent currents of Islam have been challenging the primacy of powerful nation-states and alliances, and are achieving some remarkable successes in their quest for dominance.[6]

Actually, the concept of the gray zone is not that difficult to grasp. Both modern nation states and non-state actors have also made extensive use of gray zone opportunities in the past. Soviet-Chinese-Cuban-East European support for national liberation movements and US support for anti-communist movements in Latin-America, Asia and Africa are but the most obvious examples. In the light of this fact it may be surprising that so far the western powers (and their alliances) have not managed to develop a playbook for meeting this challenge.

However, this really should not be such a surprise. First of all, in a gray zone operation, as in any other type of conflict, the belligerent who seizes the initiative has the advantage. He can apply limited and carefully metered aggression that is calculated to fall short of any recognized threshold of international war. If he overreaches himself, he can backtrack quickly, before a truly damaging military response can be delivered. Second, there is always a good deal of ambiguity regarding the nature of the conflict, the parties thereto, the appropriate legal and political framework, and the risks involved. This ambiguity is due in a good part to purposeful actions of gray zone actors, but it is also due to the organizing principles and legal and political structures of the western world. And third, perception plays a crucially important role in how the world responds.

---

5   GLOSSERMAN, Brad. Struggling with the Gray Zone: Trilateral Cooperation to Strengthen Deterrrence in Northeast Asia. Maui: Pacific Forum CSIS, 2015.

6   BESENYÖ, J. "Az Al-Kaida térnyerése a Maghreb régióban" (Al-Qaeda's increasing infruence in the Maghreb region – in Hungarian). Seregszemle, vol. VIII. No. 3. July–September 2010. 148–154. – http://www.scribd.com/doc/126275001/Sereg-Szemle-VIII-evfolyam-3-szam-2010-julius-szeptember-148-154-oldal

For example, in eastern Ukraine each principal actor perceives the conflict differently, and deploys the instruments of power accordingly.[7] For Ukraine the threat is an existential one, deep in the black zone of war: national sovereignty, is at stake, and it justifies the mobilization of all elements of national power. For Russia the situation is not nearly as acute, but the conflict is still in the dark gray area close to war, because national interests (and great power prestige) are at stake. The deployment of the information and military instruments is appropriate. NATO and the EU cannot view the conflict complacently: several member states of both organizations are threatened by Russia's potential for destabilization. Their diplomatic and economic instruments are deployed, with the information and military instruments in reserve. For much of the rest of the world (as represented by the United Nations) the conflict has been resolved by the Minsk agreement, and it is only a question of time until it is implemented fully – therefore, the situation in in the white of peace – or at most, in the very light gray area, and only the diplomatic instrument is deployed – but even that only in a cursory manner. (fig. 2.)
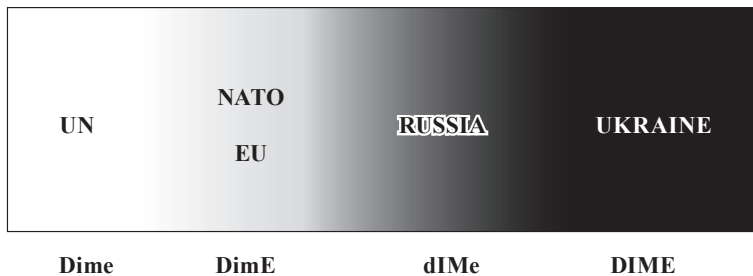
Figure 2.

Participant perception of the conflict in Unkraine. Capitalization reflects the importance each actor assigns to the elements of DIME[8]

WHAT IS TO BE DONE?

The unpredictable actions of Russia, China, North Korea and Iran seem reckless, but in reality they are carefully calculated. Being strongly centralized, autocratic states, they are better able to integrate the full range of their capabilities than

---

7   Defined by the acronym DIME (Diplomacy, Information, Military, Economic).
8   Figure drawn by the author, based on The Gray Zone.

are the western democracies, whose legal and political systems still function in a binary, either peace or war mode. As General Joseph Dunford, the Chairman of the US Joint Chiefs of Staff recently stated, "our traditional approach where we are either at peace or at war is insufficient to deal with that dynamic."[9] This suggests that in order to meet the challenge of gray zone adversaries we must adjust our legal and political structures, and our strategic vision to the new reality. We have done it in the past, and I am sure that we can do it now, and we can do it again in the future, if it becomes necessary.

Nearly two decades ago, as the Warsaw Pact was dissolved, some commentators questioned the need for NATO's continued existence in the new world order. Fortunately the member states' decision makers did not rush to judgment. They took advantage of an opportunity to reallocate some resources from defense to other priorities as the security threat seemed to diminish. With the benefit of 20 years' hindsight it is easy to criticize the decision to reduce defense spending. However, not only has NATO remained in existence, but it has also integrated new member states, and has successfully reformed itself. It has developed a new strategic vision, improved its decision making mechanism, and adopted a command structure that is appropriate for today's most likely security threats. But as the security environment is changing, we must keep pace – or better yet, anticipate the changes and meet them as they occur.

As the "War on Terror" (an unfortunate catch-phrase) unfolded, NATO nations fielded agile, light expeditionary forces that were capable of finding, fixing and fighting elusive non-state forces. Then, as hybrid threats arose, we had to adjust our focus again, to more conventional conflicts within NATO's immediate neighborhood. The Readiness Action Plan adopted at the Wales Summit in 2014 addressed these issues, but the record shows that we cannot lean back, satisfied that our job is done. Now, as the security threat shifts to gray zone challenges, we must adjust yet again our strategies and decision making mechanism.

There can be no question that technology has been hugely important in this process of continuous change, and the Alliance has been fairly successful in harnessing it. Rethinking our strategy, our decision making processes and our command structures may also help the Alliance keep pace with the changing security environment. Nevertheless, I cannot help but think that the time has

---

9   CLARK, Colin. „CJCS Dunford Calls for Strategic Shifts; 'At peace or at War is Insufficient."
     IN Breaking Defense, September 21., 2016 – http://breakingdefense.com/2016/09/cjcs-dunford-
     calls-for-strategic-shifts-at-peace-or-at-war-is-insufficient/

come to also strengthen the societal pillar of both our common and national defensive structures, and that perhaps this is more important and urgent than the reforms we have undertaken so far.

Some of us in this conference hall were already in uniform during the cold war, and we faced each other across the inner German border, or some other dividing line between NATO and the Warsaw Pact. In those years there was a national consensus in most countries about the need for a strong defense, and most countries conscripted masses of young men to field their huge Cold War armies. During the last 25 years or so most European states have suspended conscription and rely on long-service volunteers, to man the much smaller forces they need. This decision was quite popular among the young men of military age, but it has led to the development of a distinct military class that is quite separate from the rest of society. Since the threat to national security is not nearly as clear and as obvious as it was 30 or 40 years ago, the consensus about the need for a strong defense has gradually disappeared. Today few citizens feel obliged to contribute to national defense, other than grudgingly paying the taxes that support the reduced military establishments.

This attitude is detrimental at the best of times, but it is especially so today, because the gray zone challenges are often directed as much at the targeted country's inner cohesion and resilience, as against its defense capabilities, its allies, and world opinion. We have seen it happen time after time: large numbers of a troubled country's citizens are mobilized and turned against their own government by outside actors. Neither the police, nor the traditional military forces can respond adequately in such a situation. Only those nations can deal with them effectively, whose defense and stability are truly whole-of-society issues, where every citizen is part of the national defense capability in some way. "Resilience" is the current catch-phrase, and it is singularly apt in this case. Tellingly, those of our allies that are most exposed to destabilization through gray zone attacks have already taken steps in that direction by establishing territorial defense units. These contribute to national resilience by serving as something like a societal vaccination against the subversive, manipulative aspects of a gray zone attack.

Although Hungary is not a very likely target for a gray zone threat, this country also felt some of its effects, as waves of refugees from the MENA area and economic migrants from South Asia and Sub-Saharan Africa passed through the country in 2015–16. The armed forces had to be mobilized, since the police did not have sufficient reserve capacity to surge the required personnel to the border and deal with the mass of migrants at the same time.

Something like 15 percent of the Hungarian Defence Force is still deployed to patrol the southern and eastern borders. This has been a salutary, albeit unwelcome reminder, that there are security tasks that are really not the business of soldiers, but only soldiers can do them, and in order to meet them, additional manpower must be available.

The Hungarian government has taken steps to rectify the situation by creating a volunteer territorial defense force, whose units are being raised as I speak here. When they reach their authorized strength of nearly 200 companies, the number of military personnel available for handling emergencies shall have been doubled. Since these territorial forces are organized in the towns and villages of the country, and their members serve in the vicinity of their homes, they close the gap between the armed forces and society. Since they are intimately familiar with their area of operations, they also serve as societal vaccination against subversion, and thereby contribute to national resilience as well. Time will tell whether these forces are indeed as effective as their advocates claim. However, even if they are not, they are a step in the direction of enhancing society's involvement in its own defense. Should a gray zone threat materialize, Hungary would be in a better position to handle its subversion component.

THE CONSEQUENCES OF INACTION

If we insist on retaining our traditional approach of either peace or war, if we are not willing to implement far-reaching reforms in our defense establishments, and equally far-reaching changes in our legal and political structures and strategic vision, we shall have two unpalatable alternatives. Either we leave open windows of opportunity to our adversaries, thereby endangering our countries, our alliance, and the broader international community. Or we push gray zone challenges into the very dark gray or black range.

A case in point is the escalating crisis in Korea. For decades North Korea has been testing the limits of its freedom of action with small scale attacks on land and sea, driving infiltration tunnels under the DMZ, and shelling South Korean territory. It is also changing the security calculus of the whole Northeast Asia region by developing ballistic missile and nuclear capability. Meanwhile the bombastic threats of the North Korean propaganda machine do nothing to reduce the anxiety of the country's neighbors. Neither the stick economic sanctions, nor the carrot of economic aid, nor negotiations seem to

work. Time will soon tell, whether the recent robust military responses by South Korea, Japan and the United States will make the country pull back again, or military action will have to be taken to its logical conclusion. I have no doubt that if North Korea does not back down, it would be defeated, but the cost would be very high, and not only for the Koreans.

"Thinking outside the box" has become a fashionable figure of speech lately. It certainly is a valid requirement: oversimplified, outdated, formalistic operational templates are likely to lead to failure, and the deployment of additional massive firepower will not save a faulty operational design – if it ever did. However, we must not go too far in this direction: the "box" has served us well, and it still has a very important role to play. Gray zone threats are just one short segment of the spectrum of conflict. Major international war, although not very likely, is still a possibility. To remain with our Korean example, if North Korea does not back down, very large scale operations may ensue, and we need the "box" to plan and conduct them.

Ladies and gentlemen, this conference will address a significant segment of our current security environment, but one that has not been extensively studied in Europe. Even in the United States, where the term originates, it has become the subject of national security research only in recent years. However, in the light of international events, the importance of the subject is beyond question. And that brings us to the purpose of this conference.

When the General Staff's Scientific Research Center organizes an international conference, its objective is not just to create a forum to exchange views and information, gain some academic credit and build professional networks. There is some of that, of course. But a far more important objective is to find answers to current and future security threats, summarize them and present them to national and international decision makers as policy recommendations. So, I challenge you to examine the subject and debate it in light of your professional expertise. Think outside the box, but remember, that the box is a useful tool. I do not have to repeat General Patton's one-liner, because the diverse background of the participants will guarantee that you will not think alike.

PETER A. KISS is a senior researcher of the Hungarian Defence Force General Staff, Defence Research Centre. He served 26 years as a non-commissioned officer in the US Army, as parachute infantryman, intelligence specialist, psychological warfare specialist and arms control inspector. He earned his

PhD in military science at the Naational University of Public Service in Budapest in 2011. He is the author of several books, book chapters and papers in English and Hungarian on small arms, asymmetric warfare, terrorism, and military history. He can be reached at kiss.almos@hm.gov.hu.

Bibliography

BESENYÖ, J. "*Az Al-Kaida térnyerése a Maghreb régióban*" (Al-Qaeda's increasing infruence in the Maghreb region – in Hungarian). Seregszemle, vol. VIII. No. 3. July–September 2010; 148–154. – http://www.scribd.com/doc/126275001/Sereg-Szemle-VIII-evfolyam-3-szam-2010-julius-szeptember-148-154-oldal

CLARK, "*Colin. CJCS Dunford Calls for Strategic Shifts; 'At peace or at War is Insufficient'.*" In Breaking Defense, September 21., 2016. – http://breakingdefense.com/2016/09/cjcs-dunford-calls-for-strategic-shifts-at-peace-or-at-war-is-insufficient/

GLOSSERMAN, Brad. *Struggling with the Gray Zone: Trilateral Cooperation to Strengthen Deterrrence* in Northeast Asia. Maui: Pacific Forum CSIS, 2015.

KISS, Peter A. *Hybrid Warfare and Conflict in the Gray Zone.* Lecture at the Staff Officers' Military Terminology Course, Budapest, 2016.

MICHAEL J. Mazarr. *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Carlisle Barracks: US Army War College Press, 2015.

The Gray Zone. Tampa: US Special Operations Command, 2015.

WILLIAMSON, Porter B. *General Patton's Principles for Life and Leadership.* Tucson: Management & Systems Consultants. p. 151.

Spencer B. Meredith III

Governing in the Gray Zone: Reducing Strategic Vulnerabilities by Shaping the Human Domain

Abstract: This paper addresses the societal and administrative responses available to nation-states as they confront threats that focus on "society as the battlefield." At its heart is recognition of the human domain that revolves around 1) social values, 2) overlapping and sometimes conflicting identities, and 3) desired goals and methods required to achieve them. It also explores key state approaches to influence this human operational environment. In particular, the paper discusses aspects of statecraft that relate to effective governance that can build societal resistance and resilience, thereby reducing state vulnerabilities to external influence operations.

THE CHALLENGES TO THE NATION STATE

The challenges facing states today span a wide range of international and domestic factors. Focusing on geopolitics first allows analysis to draw the broader context for state actions. To begin, the concept of the Gray Zone gives key parameters for consideration. Defined in multiple ways across both geographic and specific policy issues, *Gray Geopolitics* raise several key debates. First are comparisons between the emerging international arena and past eras. Based on those assessments, it becomes possible to explore the comparative value of past geopolitical environments, narrowing down what can be applied as lessons learned vs. what remains unique to specific settings.

Second, the presence of fault lines and historic spheres of interest and influence also condition the range of state actions. Such conditions shape what is feasible along the spectrum of competition short of armed conflict, all the way to open hostilities. These shadows of the past and enduring cleavages between geographic regions do this by showing the presence of long-standing

rivalries and national security markers, which when threatened, are more likely to provoke escalatory responses.

Third, states seeking to shape human domains, both of their own countries and of others, must consider the "trip wire" of persistent interests in relation to the malleability of social values, identities, and acceptable mechanisms to promote them. Doing so highlights the role of diverse actors and actions at the global, regional, national, communal and individual levels. As all encompassing, and therefore potentially methodologically untenable as that may sound, the goal of setting the stage with all relevant actors does more than cover the analytical bases. It also reduces strategic surprise caused by unanticipated responses by adversaries, as well as previously uncommitted actors whose participation shapes outcomes in important ways.

Throughout these levels and issues, gray geopolitics remain a competition about interests as much as about values. Society has been and will likely increasingly become an engine of change, and source of pressure on states in the face of an increasingly fractured array of societal demands. At the same time, society also remains a battlefield for elite competition to "dip down" into for support in policy competitions. For example, the 2017 French Presidential election was cast as either a victory for anti-establishment populism, or its defeat by a centrist candidate. These kinds of battles are often fought as a war of words, especially among democratic polities, but not exclusively so. Even more authoritarian regimes require some consent of the governed, at a minimum of tacitly not challenging the political system or its rules.

This commonality – society as a battlefield fought with a war of words – can be seen across Europe, with contending visions for its future as much as for what Europe means as an identity itself. *Gray Europe* includes definitions tied to the European Union, NATO, partner nations, aspirants to both organizations, as well as longer-standing geographic divisions. Whether casting nations into Northern/Southern, Western/Eastern, Central/Peripheral groups, categorizations of Europe depend in part on the participants being discussed, but equally so, who discusses them and how the subject states see themselves. Across this spectrum of classifications, several questions arise dealing with what holds states together, what differentiates them from one another, and what connects Europe as a whole vis-à-vis other parts of the globe.[1]

---

1   FREDERIKSEN, M. and KNUDSEN, I. Ethnographies of Grey Zones in Eastern Europe: Relations, Borders, and Invisibilities. London: Anthem Press, 2015.

This search for commonalities, while holding to each element's uniqueness, is a hallmark of solid analysis. It allows for an appreciation of contending visions, contending interests, and contending values and identities, while also specifying cores among all three. In that regard, harmony that binds states and regions together can also include the presence of an outside "other" that makes local differences less operative. What that other is today in Europe is currently under debate though, making European political systems even more vulnerable to influence operations.[2]

DEMOCRACY – SOURCE OF STRENGTH, SOURCE OF VULNERABILITY

The heart of that vulnerability lies at the structural weakness of Europe's greatest strength – democracy. *Gray Democracy* stems from the problem of a majority of states across the world calling themselves democratic, but with an equally commensurate plurality of definitions and measurements of democracy. For example, do procedures matter more than norms or vice versa? Procedural democracy itself has a wide range of possibilities, from electoral systems that rely on rigidly based voting schedules, to ad hoc contests called by the will of the electorate. Party competition also shows great diversity as multiparty systems offer a cornucopia of choices that can easily overwhelm electorates with unclear dividing lines between parties, while single or bipartisan systems can include internal factions that do the same things.

Separation of powers between rival institutions can also be a source of strength as well as a vulnerability, with fundamental questions of who gets which responsibilities morphing into gridlock, as often as checks on abuse of power by one or more institutions occurring. Underlying this is the rule of law, which itself raises questions of immutability vs. responsivity on issues defining everything from citizenship to civil rights. In addition to the mechanisms by which those rights are protected, there is also the factor of potentially expanding them as well. The ebb and flow of these two contradictory trends is a hallmark of democratic governance. Therefore, inherent to democracy is the necessity of boundaries that are both predictable and not easily changed,

---

2   BARGIACCHI, P. "The EU Strategy for Democracy in Libya and Ukraine: Legalizing Human Security or, Rather, Promoting the ‚European Way of Life' in the Wider World?" Paper Presented at the International Conference „Researching Security – Approaches, Concepts and Policies", Ohrid, 2–3/6/2015.

while also being adaptable and responsive when necessary. The lack of absolute analytical definitions makes these systems at times both strong and vulnerable.

This is even more apparent when considering the normative aspect of gray democracy. Social contracts form a pillar of democratic governance, but the values undergirding that pillar can and often do face pressures to change if the system survives long enough. As seen in the battle over religious rights and discrimination in the United States, key questions arise as to who is "forcing" the change on whom, and through which of the democratic political institutions at stake. Contending paradigms of government accountability arise in these contexts, as they also do in cross-cultural comparisons and foreign policy interventions. However, despite these normative debates, one aspect still remains at the center of democratic governance – the responsibility for self-government inherent to the name itself. As *the* core for this type of political system, it can serve as a universal measurement that can include cultural nuances as well.

Responsive government balances the other side of the democratic equation. With citizens fulfilling their role in holding governments accountable to their election promises and the underlying rules of the political game, responsivity by said government enables the system to weather diverse storms that threaten it from the range of gray conflicts mentioned thus far. Accordingly, *responsivity centers on defining and defending the space for public debate.* Focused on the types of issues, as well as more basic questions of who gets to debate what, in which manner, and when and where all of this can take place, responsivity is fundamentally rigid. Yet it is equally malleable in that change can and must occur to the boundaries of debate, but the key must be that such changes occur relatively infrequently and within the rules of the game. Therefore, responsivity can be found within authoritarian regimes as well, even if the malleability and number of participants in the change process are significantly reduced compared to democratic systems.

As a result, this kind of *government responsivity defines the human domain*. It shapes and is shaped by narratives that give meaning to events and the actors who participate in them. It also shapes and is shaped by external changes in the context of governance, whether through social, economic, or political factors at multiple levels of actions across the international and domestic spectra. Relying on this concept thus allows analysis to engage cultural nuances that make democracy work in different places, thereby highlighting the greatest strength of democracy as a concept and practice – *Effective Governance*. This

becomes one of the key elements for inoculating populations from hostile influence operations.

The Key – Effective Governance

Effective governance gives states a form of soft power to influence both domestic and international audiences. It uses three primary modalities. First is the principle of attraction. The "city on a hill" neither moves locations to convince others of its merits, nor does it force others to join it. Rather, it beckons outsiders to come and follow its examples by means of its success and appeal to common collective goods. These are also two of the historical realities of long-standing democratic polities – security and prosperity – despite the presence of lapses along the way. Yet, city leaders also have a secondary responsibility to "shape opinions" in the contests within the communal boundaries of debate, as well as without the city among the contending messages and lures for their populations' attention and affection. Winning this war of words relies in part on the third strategy of "naming and claiming" that uses narratives to set the terms of debate, as much as the conditions for success and failure. Each of these strategies support and need each other, just as they rely on elements of hard power to back up both capacity to deliver collective goods and deter aggression. Three European examples offer distinct pictures of each of these factors at work, with nuances around a core of key concepts and practices.

Poland has a core of interests that center on increasing its role and prestige internationally, while also working to further European integration. Both are meant to enhance the country's security and prosperity, and are focused internationally while being reinforced domestically. Supporting those through intentional messaging, Poland emphasizes the narrative of a successful democratic transition that has become a vital economic and security partner to the region. Several mechanisms to "reach out and bring in" include development aid to parts of Eastern Europe; Russian language TV, radio, and internet services sponsored by the government; cultural festivals in neighboring countries; and education scholarships to bring students and

professors to Poland.[3] Each seeks to show the success of Poland's movement from its communist past by means of responsive, effective governance.

Lithuania shares similar interests, but with a greater emphasis on preserving the country's territorial and functional independence. Its primary message focuses domestically, but is also reinforced internationally. As such, it highlights a unified democratic nation with a thriving capitalist economy that is both vital to NATO and under threat from Russian aggression. The mechanism to "dig deep and hold ground" builds honor for and knowledge of the country's historic struggles for independence through school curriculum and national symbols. Equally important are efforts to strengthen civil society and build bridges to diverse communities through close ties with the national military.[4] This institution serves as both a cohesive, unifying national identity marker, as well as a reminder of the heightened threat from Russia. Like Poland, Lithuania's reference to its successful democratic system reinforces governance as a means to inoculate the population from divisive external influence operations.

Finland follows that model with even greater cohesion between security and democratic governance. With clearly stated interests to prevent Russian hybrid activities, Finland has taken up the mantle of communicating that threat broadly within the European region. The message remains simple yet poignant – the functional pillars of effective Finnish governance are capable of building resilience within its society. Democratic rules and procedures, alongside an effective bureaucracy that delivers collective goods while remaining accountable to election results, give legitimacy to both the interests at stake, as well as the means to ensure them. Messaging supports this process by showing that information warfare is common and persistent, and that its success depends on shared languages, histories, cultures and ultimately, a willingness to buy into it. These different vulnerabilities and sub-domains within the broader human domain, do not by themselves mean success for Russian influence operations. The Finnish message also highlights the catastrophe of the Donbas as a more likely scenario for further Russian aggressions, rather than the comparatively placid Crimean annexation.

---

3   SADOWSKI, R. "Poland's Soft Power in Eastern Europe" in Rostoks, T. and Spruds, A. (eds), The Different Faces of "Soft Power": The Baltic States and Eastern Neighborhood between Russia and the EU. Riga: Latvian Institute of International Affairs, 2015, 64–79.

4   MURAUSKAITE, E. "Lithuanian Security Culture: Insights on Handling Gray Zone Threats". Paper Presented at START National Consortium for the Study of Terrorism and Responses to Terrorism, Washington, 28/2/2017.

Finland also has a broad security-society connection based on the concept that there are "many seats at the democratic table; all have responsibilities" to participate and protect the polity. This security strategy for society includes cooperation between multiple government agencies and social groups, as well as interagency coordination to ensure harmony of efforts. These allow for a spectrum of proactive planning methods, all the way to crisis management. Supporting these activities located primarily in the political arena, national defense education engages society at the fundamental level with the goal of improving comprehensive security and psychological resilience.[5] Conscript training and short courses for professionals in a variety of vocations also gets the message out to a wide audience, and equally importantly, allows for responsive governance by reversing the information pipeline. By creating regular, predictable conduits for communication between state and society, Finland's approach emphasizes effective governance as the core of inoculating its population against hostile influences.

Taken as a whole, these three brief country examinations indicate areas of successful governance and messaging. They do so in multiple gray contexts, which is no easy task given that the pressures arising across those areas are often contradictory, persistent, and highly adaptable. However, rather than chasing after solutions to each problem individually, and instead focusing on the core of responsivity as a means to effective governance, democratic countries can more than simply match threats from hostile influencers. They can also successfully reduce their strategic vulnerabilities in the human domain, something increasingly necessary as the Gray Zone looks to become the dominant paradigm of international and domestic politics for the foreseeable future.

> Spencer B. Meredith III, PhD is an Associate Professor of National Security Strategy at the U.S. National Defense University (NDU). He previously served as a Fulbright Scholar in the Caucasus working on democratic development and conflict resolution, and has focused on related issues in Central and Eastern Europe for several years. He has also served as a subject matter expert for US Department of State public diplomacy programs dealing with the role of religion and

---

5   PUISTOLA, J. "Finnish Comprehensive Security Concept in Response to Gray Zone and Hybrid Threats." Finnish Defence Forces, Secretariat of the Security Committee. 3/12/2016

democracy in US foreign policy. Dr. Meredith has advised US Special Operations Command projects on countering Russian influence operations in Ukraine and the Baltics, US Central Command programs analyzing and supporting effective governance in Iraq and Syria, and other US Army Special Operations efforts in analyzing narratives, deterrence, and a range of violent and non-violent conflicts. He has published widely in his areas of expertise in comparative and international politics. He can be reached at: spencer.meredith@gc.ndu.edu.

BIBLIOGRAPHY

BARGIACCHI, P. "*The EU Strategy for Democracy in Libya and Ukraine: Legalizing Human Security or, Rather, Promoting the 'European Way of Life' in the Wider World?*" Paper Presented at the International Conference "Researching Security – Approaches, Concepts and Policies", Ohrid, 2–3/6/2015.

FREDERIKSEN, M. and KNUDSEN, I. *Ethnographies of Grey Zones in Eastern Europe: Relations, Borders, and Invisibilities.* London: Anthem Press, 2015.

MURAUSKAITE, E. "*Lithuanian Security Culture: Insights on Handling Gray Zone Threats*". Paper Presented at START National Consortium for the Study of Terrorism and Responses to Terrorism, Washington, 28/2/2017.

PUISTOLA, J. "*Finnish Comprehensive Security Concept in Response to Gray Zone and Hybrid Threats*". Finnish Defence Forces, Secretariat of the Security Committee. 3/12/2016

SADOWSKI, R. "*Poland's Soft Power in Eastern Europe*" in Rostoks, T. and Spruds, A. (eds), *The Different Faces of "Soft Power": The Baltic States and Eastern Neighborhood between Russia and the EU.* Riga: Latvian Institute of International Affairs, 2015; 64–79.

MOLLY NADOLSKI

A Framework for Complex Systems Analysis of Gray Zone Conflict

Abstract. Despite strides in techniques for assessing problem spaces, using risk management, network science, or development tools, our collective understanding of increasingly complex domains remains nascent. In the study of Russian foreign and security policies specifically, the limitations of the theoretical frameworks, statistical, and qualitative methods for testing theories of strategic interaction and comparative foreign and security policies are conspicuous. This paper introduces an analytical framework and toolset that decision makers can use to assess complex systems, using the case study of Russia's application of gray zone tactics in Moldova and Georgia. The toolset enables decision-makers to analyze how best to intervene in ever-changing complex systems.

Introduction

Most pressing social problems do not have obvious or ready solutions. This is largely due to the complexity of the world in which we live. To understand if there is the potential for long-lasting change within a problem space, decision makers must contend with this reality. One cannot hope to fully represent the complexity inherent in large-scale social problems; there are too many interactions and unknowns. However, using a suite of systems analysis, strategic foresight, and data integration tools, we can better visualize these complex problem spaces and clarify some, if not all, of the interacting forces at play. In today's world, many complex systems are undergoing transformations that are difficult to explain or predict using conventional methods of analysis. The United States Department of Defense (DoD) implements the term VUCA (volatility, uncertainty, complexity, and ambiguity) to describe the environment of strategic leadership. Further expanding on the term,

Harry Yarger characterizes the strategic environment as being vulnerable to rapid changes, "inherent instability", and prone to multiple conflicting interpretations. The author also describes complexity as "many parts that are intricately related in such a manner that understanding them collectively or separating them distinctly is extremely difficult and often impossible."[1] As Dale Moore points out, research has been conducted on sensemaking in relation to knowledge structures, schemas, and mental models.[2] He emphasizes, however, such research has not focused on its relationship to the formation of strategy, particularly in relation to complex environments. When applying the VUCA framework within the environment of international relations and security, it becomes clear that the unpredictability in this context may hinder our understanding of the environment, leading us to come to misguided conclusions, which would result in erroneous policy implementations. What's more, the consequences of ill-advised policies could lead to costly long-term negative effects, further muddling the already complex environment. Clear understanding of the degree of complexity is necessary in the process of decision-making and policy development. In his book "Ontology Alignment", Marc Ehrig describes the necessity to create an integrated platform for greater understanding of information between various domains; he writes "to foster understanding in new semantic technologies, data integration, and the interaction between the two fields … goal is not to align ontologies by only integrating the syntax, but actually bringing together entities which have the same meaning, thus bridging the semantic gap."[3] As such, it is important to keep in mind the meaning that is underlying the information.

Therefore, the assessment of a complex system and related policies have to explore the holistic makeup of the system (i.e., its components), the interactions within (the ties among the individual elements, strengths/weaknesses and behaviors of specific "nodes", opportunities and fault lines associated with each), as well as the opportunities and risks relevant to the main question of interest or goal of the system (i.e., accounting for the unique elements of the scenario at hand as well as for specific outcomes we are looking to achieve).

1   YARGER, Harry Richard. Strategy and the national security professional: strategic thinking and strategy formulation in the 21st century. Greenwood Publishing Group, 2008.
2   MOORE, Dale L. The Experience of Strategic Thinking in a Volatile, Uncertain, Complex, and Ambiguous (VUCA) Environment. Dissertation. George Washington University, 2014.
3   EHRIG, Marc. Ontology alignment: bridging the semantic gap. Vol. 4. Springer Science & Business Media, 2006.

Applying a Complex Systems Approach to Gray Zone Conflict

Although there are numerous theoretical frameworks, statistical and qualitative methods for testing robust theories of strategic interaction and comparative foreign and security policies, most use only individual data sets and do not address multiple and complex interactions across issue areas and actor-types in related problem spaces. In order to contend with complexity and generate forecasts relevant for policy analysis, it is necessary to broaden, integrate, and augment existing and novel methods and approaches. Furthermore, few efforts have been made to translate emerging research in these approaches into user-friendly and interactive visual tools that can aid in both hypotheses generation, strategic forecasting, and scenario assessment.

These limitations are especially conspicuous in the study of Russian foreign and security policies. Here, the conventional focus on single-factor explanations has been challenged by the emerging cross-domain character of Russia's statecraft and pursuit of so-called "new generation warfare" in gray zone conflicts. Gray zone conflict is defined as the "purposeful application of multiple elements of power—information, economic, military, political—to achieve objectives in ways that exceed the threshold for normal competition yet fall below the level of major interstate war."[4] As a complex system highly characterized by multi-levels and multi-attributes, this warrants an analytical approach specifically designed to address these needs and capabilities, as such, we need to evolve our approaches and processes. However, the field is dominated by the application of a narrow set of research methods, such as comparative case studies, regression analysis, expert surveys, and interviews that confront systematic problems related to limited, out of sample, and disconnected data. This is all the more challenging, as there are a growing number of coding software and tool-sets that offer opportunity to automatically extract stakeholders, sentiments, and events related to foreign and security policy analyses from a growing body of English and Russia (and other languages) databases and media publications on daily and even real-time bases. Together, these present gaps in understanding the links between the Russian leadership's stated objectives, preferred tools and strategies for exerting multiple elements of power and influence; Russia's actual foreign and

---

4 „Foreign Approaches to Gray Zone Conflicts." NSI. National Intelligence Council, Mar. 2016.

security behavior, and the Kremlin's effectiveness at implementing preferred cross-domain policy instruments and achieving its desired ends.

As such, this research addressed these gaps and created an analytical framework and toolset that decision makers can use to assess complex problem spaces, using the context of Russia's application of gray zone tactics. This customizable toolset assessed the current and future impact that decisions, policies, or strategies can deliver in a system to tackle particularly complex problems. Being empowered with the appropriate toolset enables decision-makers to analyze how best to intervene in ever-changing complex systems. Beyond providing decision-makers and policy-makers with stronger analytical capabilities and holistic conceptual toolset, this research approach has had several other outputs as well:

1. **Ontology resolution:** Given the multi-disciplinary nature of the gray zone conflict domain, it required reconciling vernacular and ontological differences between the fields. Often, subject matter experts use different words to describe the same phenomena, or the same words to describe different phenomena. This research sought to create commonalities or resolutions in addressing these ontological challenges when possible.

2. **It exemplified the need for more systematic and formal integration of systems thinking tools and frameworks that specialize in dealing with complexity**: This is especially true in social science domains and international affairs. Further, it presents a formal design process that can bring together different groups and teams.

3. **Eliminate and/or reduce bias, embedded assumptions, and competing viewpoints.** In many cases, models are generally accurate within one aspect of the system, but the assumptions put into the models reflecting other aspects are incorrect or no longer valid. In complex domains, competing viewpoints or bias can hinder stakeholder collaboration and decision-making. Frameworks that include participatory and collaborative modeling reduce the influence of these factors.

4. **Bridging qualitative and quantitative methods.** Often, these are treated as discrete or mutually exclusive domains. By establishing a multi-method and multi-tool approach, this research goes beyond simply identifying qualitative and quantitative tools available. Rather, it seeks to create bridges between them and connect their application for a fluid and cohesive research process, in which their output and design relate to one another for a truly cross-disciplinary approach.

Toolset Elements

The novelty of applying a toolset approach is that it does not rest in a single theory, analytical method, tool, or a unique dataset. Rather, it rests in a rigorous methodology for an iterative process that involves a wide mix of subject matter experts to create a toolset that explores multiple research questions, datasets, and analytical tools over time. This will provide decision-makers with a "playbook" for decision-making strategy and conducting research. The toolset included a number of tools that help to clarify the boundaries of the problem space that define the situation in question (or the system in which the problem— such as Gray Zone Conflict — occurs) for which decisions or political strategies are sought. A problem space could be Russia's intervention in Ukraine, or the ongoing conflict in Syria. Beyond the description of a problem, a problem space includes the various stakeholders, policy drivers, institutions, and other features that define the system in which the problem occurs.

Figure 1.
Key Toolset Elements
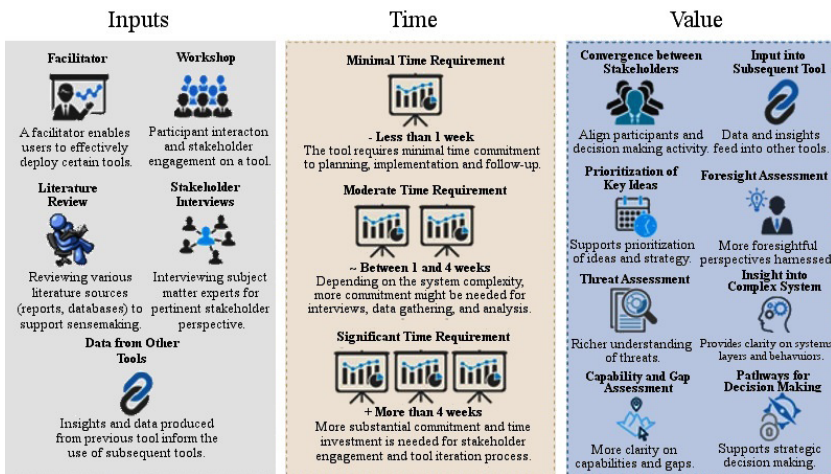
The survey broadly collected, analyzed, and organized the tools and insight curated in the project into a well-maintained, multi-user resource. Figure 1 shows the delineation of key toolset elements of the methodological approach. To define such a methodology, the research project considered: What inputs (data from other tools, facilitator, workshop, literature review, and interviews)

are required to run each tool? How much time (days/week) is needed? What type of value results (convergence between stakeholders, input into subsequent tools, context insight, futures insights, prioritization of key ideas)?

Navigating through the toolset offers a research-based journey during wherein some tools can be performed through desk research and interviews, while others best occur through a facilitated workshop. Broadly, this toolset is designed specifically to aid in focused research activities beyond the selected context, such as broader security and defense related challenges. In this sense, it is novel, as few such frameworks exist. However, the applied case study is important: current analyses of Russia's external strategy and behavior typically employ narrow research methods, sources, and tools. Furthermore, doing the legwork to distinguish value-added tools from those that offer little despite their time- or resource-intensity, we will be able to identify new ways for expanding the empirical and analytic bases for generating practical understanding of different complex problem spaces related to Russia's international behavior.

Toolset Application

The initial phase of the project effort began with a comprehensive scan of conceptual tools and soft systems methods currently used to visualize or model complex problem spaces. It involved a cross-disciplinary literature review and data search to identify tools and theoretical frameworks stemming from risk management, development, economics, social planning, cognitive science, political science, systems engineering, and more. The project identified those best suited to provide value insight in this domain, according to user and toolset needs. The project identified 33 conceptual tools, 16 theoretical frameworks, and 15 computational tools, which informed toolset design, focusing on those that can be structured around strategy and visualizing unstructured spaces, such as gray zone conflict. The identification is accompanied by a taxonomy that depicts their unique use, function, and capability as shown in figure 1, wherein users can select which tool will meet with data needs, time/resource requirements, and value output to feed into a "playbook" approach for decision-making. The visualizations also help shape strategy and reach understanding in an unstructured domain.
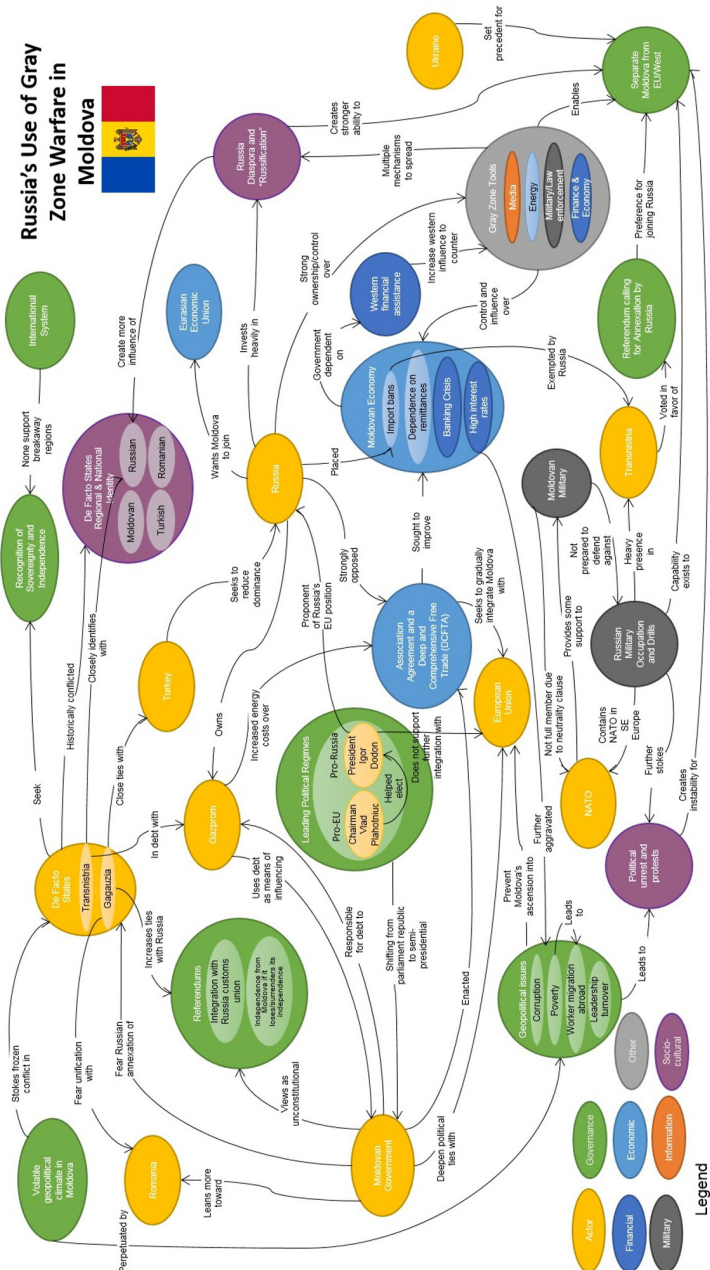
Figure 2.
Example Systemigram of Gray Zone tool Used in Moldova

The project selected three tools to be tested against the scenario of Russia's application of gray zone tools in Moldova and Georgia. These tools were: Systemigram, Problem and Objectives Tree Analysis, and Stakeholder Influence Mapping. These were selected according to their unique function, design, and output. Narratives that described the scenarios were produced which would inform toolset selection and be used as data inputs into the model design. Figures 2, 3, and 4 show an example of each tool used applying the Moldova case study. Each tool provides a unique visualization of the problem space, with differing designs the reflect relationships, activities, and behaviors, along with complementary value output to optimize holistic strategy development and insight validation.

Figure 2 shows a systemigram, a systems diagram, which captures processes, behaviors, emerging trends, interactions, interdependencies, uncertainties and gaps, for a multi-level representation of the problem space, in a single picture. This is usually difficult to do in complex problem spaces and a capability that often lacks in existing models. This makes it a particularly powerful tool to use, especially for modeling gray zone conflict and the differing applications of gray zone specific tools. These tools also provided visualizations of the outcomes and processes, which were then presented to subject matter experts to confirm and verify the findings of the tools. This created an iterative design process and reduced the possibility or bias or assumption-placing when capturing the problem space.
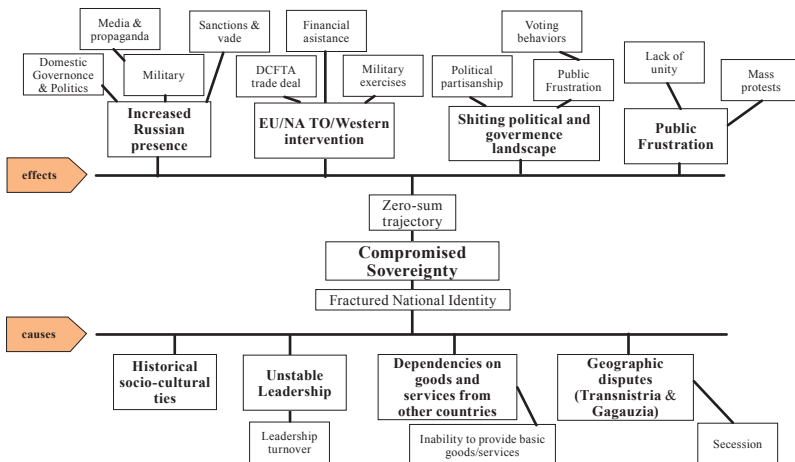

Figure 3.

Example Problem Tree Model of Compromised Sovereignty in Moldova

Figure 3 is an example visualization from the Problem and Objectives Tree tool. This allowed the research to highlight the root/fundamental problems and objectives, while branches helped visualize consequential objectives.[5] Figure 4 shows an example diagram of the Stakeholder Influence map, which was useful as an aid in capturing the influence and power of specific stakeholders in relation to policy measures. Stakeholder influence mapping helps expose what brings about change in decisions and prevailing wisdom over time, and how they might be shaped in the future.[6]

Moldva Economic Policy *Current* Stakeholder Influence
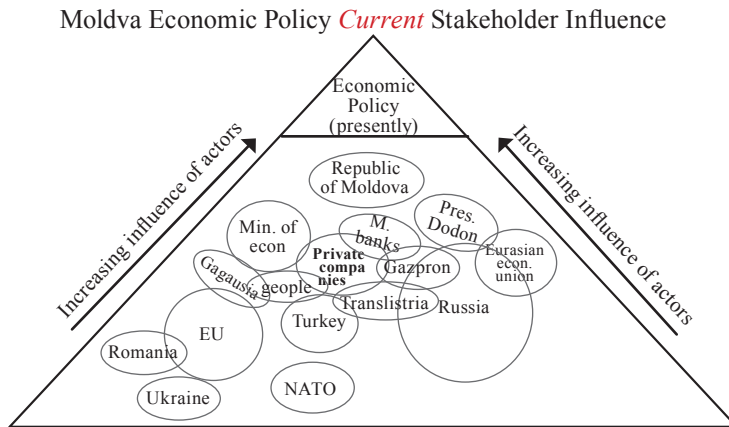
Figure 4.
Example Stakeholder Influence Map of Economic Policy in Moldova

Using these additional tools, the finds were validated that stemmed from the systemigram. Together, they revealed the prominent role that the Eurasian Economic Union played in driving Russian behavior in the region and "zero-sum" position of the Moldovan government in terms of Russia-EU bilateral relations. Russia's tactics and strategies were mapped, and specific use of gray zone tools were categorized and captured to visualize how they interacted and/or influenced the problem space. From this, we are able to derive some of the numerous complex factors that might be driving Russia's behavior, the role key stakeholders and governments play, gray zone tool application, and understand competitive strategies versus tactics. Overall, these three

5   Tools for Development: A Handbook for Those Engaged in Development Activity. Department for International Development. Mar. 2003.
6   MAYERS, James and VERMEULEN, Sonja. Power Tools: Stakeholder Influence Mapping. International Institute for Environment and Development, 2005.

conceptual tools provided very strong and nuanced perspectives of the problem space, which otherwise would have been difficult to visualize and not captured elsewhere in literature searches.

Conclusions

Few efforts have been made to translate emerging research in these approaches into user-friendly and interactive visual tools that can aid in both hypotheses generation, strategic forecasting, and scenario assessment. Furthermore, there is very little literature on modeling gray zone conflict using various modeling methods. To create a holistic approach and toolset, this research draws on theories and frameworks from multiple disciplines that developed approaches and techniques for problem solving, decision-making, and strategy. It provided a comprehensive set of tools and frameworks that allows individuals from diverse backgrounds to address a variety of questions and to delve into the complexity of each situation without the loss of time and resources otherwise spent on the search for and implementation of the appropriate problem-solving method. In addition, these tools are specifically designed and selected to address complex problem spaces, and take into consideration the unique characteristics, transformations and behaviors that drive these domains and needs to be captured in visualizations. These existing tools were augmented and tested to uniquely address the case study of Gray Zone tactics used in Moldova and Georgia. This provided a thoroughly documented approach for conducting research and documenting strategy for a playbook approach to decision-making.

By developing such a toolset, this supports interdisciplinary thought leadership across campus for collaborative learning, by guiding definition of shaped future scenarios and accompanying action plans. It can be utilized to develop a "decision arena" to convene stakeholders in order to play out possible futures in a data visualization arena. Furthermore, this project seeks to build off the toolset more to connect the qualitative tools to quantitative tools. Designing data analytic and computational models that accurately reflect performance measures at different layers of society, and the aggregation of measures from one layer to the next, remains a fundamental issue in developmental and policy practice. By bringing in other approaches and novel methods, such as complex systems analysis tools, systems dynamics

and big data, this will allow us to probe new hypotheses, capture macro-level behavior, and model semantics.

Molly Nadolski leads policy research at Georgia Tech Research Institute in Atlanta, GA, USA, conducting thorough qualitative analyses, problem-space modeling, and applying systems thinking to explore complex enterprises. Her research interests include socio-technical and socio-cultural issues related to security and defense, international conflict, geopolitics, cyberspace, and resilience. Prior to her position at GTRI, she worked at several consultancies in Brussels, Belgium that carried out EU funded projects focused on technology, innovation, and security. Molly received her Master's degree (M.Sc) from Vrije Universiteit Brussel (Brussels, Belgium) in Political and Social Science with a concentration on cyber security, and an undergraduate degree from Vesalius College (Brussels, Belgium) in Political Communication and Public Diplomacy. She can be reached at molly.nadolski@gtri.gatech.edu.

Bibliography

"*Foreign Approaches to Gray Zone Conflicts.*" NSI. National Intelligence Council, Mar. 2016.

EHRIG, Marc. *Ontology alignment: bridging the semantic gap.* Vol. 4. Springer Science & Business Media, 2006.

MAYERS, James and VERMEULEN, Sonja. *Power Tools: Stakeholder Influence Mapping.* International Institute for Environment and Development, 2005.

MOORE, Dale L. *The Experience of Strategic Thinking in a Volatile, Uncertain, Complex, and Ambiguous (VUCA) Environment.* Dissertation. George Washington University, 2014.

Tools for Development: A Handbook for Those Engaged in Development Activity. Department for International Development. Mar. 2003.

YARGER, Harry Richard. *Strategy and the national security professional: strategic thinking and strategy formulation in the 21st century.* Greenwood Publishing Group, 2008.

Imre Porkoláb

NATO's future vision for fighting in the Grey Zone: a Persistent Federated Approach[1]

"The war you prepare for is rarely the war you get"[2]

Abstract: The presentation focuses on our organizational and leadership methods, which are quickly becoming obsolete in the contemporary context. It will cover three areas (1) a quick introduction of the main problems associated with contemporary Grey Zone Conflicts (2) A theory of the contextual approaches (3) NATO's vision for organizational transformation in a VUCA environment, and the leadership approaches and operations associated with this vision. The main theories presented will be a framework to better understand the VUCA context, NATO's Persistent Federated Approach, and Complex Adaptive Leadership. The presenter's thesis is that a VUCA context preclude direct hierarchical-bureaucratic supervision and leadership must focus on the expertise of decentralized teams with selective skill-sets and experiences, as well as creating a shared situational awareness. Overall an integrated approach to leadership and organizational transformation will be presented, suggesting that understanding, developing and practicing an integrated approach will better prepare all leaders to handle difficult situations in complex operations.

2   KRULAK, V. (1984). First to Fight: An Inside View of the U.S. Marine Corps. Annapolis: Naval Institute Press, Ch12.

INTRODUCTION

NATO transformation seems to be on the forefront of the agenda on both sides of the Atlantic. During a recent NATO Secretary General visit to the US President Trump reaffirmed the strong commitment of the United States to NATO, and the value he places on the transatlantic bond in general, and stated that the Alliance "it's no longer obsolete."[3] In Brussels NATO leaders also understand that the Alliance must adapt in response to the new strategic reality. In early February 2017 Defense Secretary Jim Mattis said during a press conference after the Defense Ministerial meeting that he and the ministers had considered in detail the strategic situation facing the Alliance. *"We thoroughly discussed the increased threats facing our alliance and, unified by the threats to our democracies, I found strong alliance resolve to address these growing threats."*[4]

The Defence Secretary also participated in the Munich Security Conference, where he emphasized the importance of NATO's Allied Command Transformation: "*NATO has only two Supreme Allied Commanders: such is the importance NATO places on adaptation, that one of those two commanders is assigned the sole mission of charting NATO's constant Transformation.*"[5] Mattis pointed out that NATO must focus on adapting the Alliance to new challenges such as terrorism, cyber threats, and hybrid war.

The Chairman of the Joint Chiefs of Staff, Gen. Joe Dunford also spoke about strategy during a session at the Brookings Institute where he said that it is important that the alliance continue to transform, *"to be relevant for the threats of today and tomorrow"*.[6]

In line with that reasoning NATO held its Transformation Seminar on 23 March 2017 in Budapest, Hungary, hosted by the Hungarian Minister

---

3   BENNETT, Brian. "NATO 'no longer obsolete,' Trump says after meeting with alliance chief," Los Angeles Times, Apr. 12., 2017 – http://www.latimes.com/politics/washington/la-na-essential-washington-updates-despite-calling-nato-obsolete-trump-1492008895-htmlstory.html
4   PELLERIN, Cheryl. "Mattis: NATO is Evolving in Response to New Strategic Reality." DoD News, Defense Media Activity. Feb. 16., 2017 – https://www.defense.gov/News/Article/Article/1085796/mattis-nato-is-evolving-in-response-to-new-strategic-reality/
5   MATTIS, Jim. "Remarks by Secretary Mattis at the Munich Security Conference in Munich, Germany." US DoD, Secretary of Defense Speech, Feb. 17., 2017 – https://www.defense.gov/News/Speeches/Speech-View/Article/1087838/remarks-by-secretary-mattis-at-the-munich-security-conference-in-munich-germany/
6   GARAMONE, Jim. "Dunford Discusses Strategy, Threats at Brookings Event". DoD News, Defense Media Activity. Feb. 23., 2017 – by https://www.defense.gov/News/Article/Article/1093155/dunford-discusses-strategy-threats-at-brookings-event/

of Defence István Simicskó. The Seminar's main theme, *Charting Alliance Adaptation* provided a forum for the political and military leadership to discuss the Alliance's need to continuously adapt in order to defend against emerging security challenges. NATO's transformation paradox was articulated by Deputy Secretary-General Gottemoeller, who said that *"NATO not only needs to spend more, we need also to spend better. And Allied Command Transformation helps us to spend better."*[7]

The statement that triggered this paper was communicated by SACT, General Mercier, who in his opening speech emphasized that NATO needs to operate and adapt at the same time, and it is a wicked problem for the Alliance. In this paper I would like to dig deeper into SACT's problem statement, and present a vision of a transformation strategy for NATO in the so-called Grey Zone, a persistent federated approach, which can be a potential answer to the Alliance's transformation paradox.

FIGHTING IN THE GREY: UNDERSTANDING THE CONTEXT IN A RAPIDLY CHANGING SECURITY LANDSCAPE

Analyzing the last couple of hundred years, we can realize that the majority of conflicts in fact, fall between the traditional duality between war and peace and are characterized by ambiguity, uncertainty and volatility, the so called Grey Zone.8 What is this Grey Zone, and how can we define it?

A recent study surveyed multiple conceptualizations and suggests that although there is common understanding of war and peace, it is less

---

7   GOTTEMOELLER, Rose. Speech at the NATO Transformation Seminar, Budapest, Hungary, Mar 23., 2017.

8   The Gray Zone is a term mostly originated in the US Special Forces community. Examples of academic articles on this topic include: VOTEL, Joseph L. – CLEVELAND, Charles T. – CON-NETT, Charles T. and IRWIN, Will. "Unconventional Warfare in the Gray Zone." Joint Forces Quarterly, 2016/1.; Gray Zone. U.S. Special Operations Command White Paper. Tampa: USSO-COM, Sep 9 2015.; BARNO, David and BENSAHEL, Nora "Fighting and winning in the Grey Zone." War on the Rocks, May 19., 2015; BRANDS, H. "Paradoxes of the Gray Zone." FPRI. Feb 5., 2016 – http://www.fpri.org/articles/2016/02/paradoxes-gray-zone; ELKUS, A. "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense." War on the Rocks, Dec 15., 2015 – http://warontherocks.com/2015/12/50-shades-of-gray-why-thegray-wars-concept-lacks-strategic-sense/; "Not at Peace and Not at War: An Exploration of "Gray Conflicts." Joint Strategy Review Study. 2015; MAZARR, M. J. Mastering the gray zone: understanding a changing era of conflict. Carlisle: Strategic Studies Institute, Army War College Press, 2015 (Advancing Strategic Thought Series). http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1303.

understood what fall in between them.[9] The academic community seems to be in agreement that Grey Zone conflicts are aggressive in intent and serve a broader strategic objective. There is also a general consensus that they use multiple forms of power to pursue their ideological or political goals, which render a militarized response inappropriate and muddles the response options. Nearly all discussions of the Grey Zone mentions ambiguity and uncertainty, which seem to be the defining characteristics of this type of conflict.[10]

Based on the above it is obvious that NATO is very much interested in this topic, as it seems to be in contrast to linear military campaign models, disrupts the risk calculations, persistently complicates decision-making, force calculations and traditional deployment approaches, and overall creates strategic uncertainty. Developing a common, compelling and adaptive strategic approach, which is actionable and can be implemented in a rapid manner is essential. One thing is clear: the current NATO joint phasing model seems to be inadequate to seize and maintain the initiative in the Grey Zone, so we need something different.[11]

The other frequently asked question is how often we find ourselves in this uncertain situation just short of our understanding of war. The Correlates of War project at the Pennsylvania State University for example has looked at every war since the Napoleonic Era and researchers used this database to categorize the nature of war.[12] The outcome of their findings was that less than 20 percent of all wars have been traditional (state-on-state) and the remaining 80 percent fell into the irregular (grey) category.

9   BRAGG, Belinda "Specifying and systematizing how we think about the Gray Zone." NSI, Jun. 27., 2016 – http://nsiteam.com/specifying-and-systematizing-the-gray-zone/specifying-and-systematizing-the-gray-zone/

10   JOBBAGY, Zoltan: "Effects-Based Operations and the Age of Complexity: A Critical Reflection." Militaire Spectator, May 2006; pp. 235–242.

11   This statement can be found in a report sponsored by the ARCIC in coordination with US JoInt Staff J-39 Strategic Multi-Layer assessment Branch. The project director was Nathan Freier with multiple contributing authors. Outplayed: Regaining the initiative in the Grey Zone, Carlisle Barracks: Strategic Studies Institute, United States Army War College Press, 2016; pp. 17 and 98–99.

12   GORKA, Sebastian and KILCULLEN, David "An Actor-centric Theory of War: Understanding the Difference Between COIN and Counterinsurgency," Joint Force Quarterly, 2011/1.
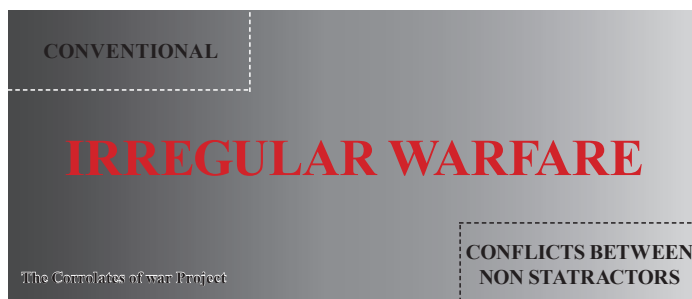
Figure 1.
Distribution of warfare based on the correlates of war project data.[13]

The reality on the battlefield suggests that what we call conventional or traditional warfare is, in fact, a rare phenomenon and we mostly find ourselves fighting in the Grey Zone, where the Westphalian military ethics and the Clausewitzian rulebook are not applicable. Moreover, if we look at most NATO countries' professional military education, they mostly focus on teaching traditional warfare methods and strategies and very little time is being spent on educating the force on the art of war as it applies to the apparently most prevalent form.[14]

The challenges in the Grey Zone can be many, but there seems to be an understanding that while the Westphalian construct can clearly understand war and peace and how to act during these instances, in the grey perspectives matter, ambiguity clouds judgement and adversaries can achieve success by taking purposeful action in the vacuum of our clear understanding. During these times, non-state, or proto-state actors (supported by nation states) can gain advantage over entrenched governmental bureaucracies.[15]

---

13   The figure was inspired while watching a panel discussion of intelligence experts in Jan 2017 in Washington DC debating the challenges of future warfare, followed by a presentation of Sebastian Gorka, NSC adviser to the US President. Data depicted ont he figure has been sourced from: Gorka and Kilcullen. "An Actor-centric Theory of War."

14   BAKOS, Csaba Attila; FARKAS, Sándor: Gyakorlatorientált oktatás, képzés és kiképzés, avagy a pályaszocializáció a katonai felsőoktatásban, Honvédségi Szemle, 2016/4; pp. 85–86.

15   See for example the Sahrawians (backed by Algeria and Libya) fighting against Morocco and Mauritania in the Western Sahara, or the Zaghawa rebels, strongly supported by Chad, fighting against the Sudan government's forces in Darfur. BESENYŐ, János "The Occupation of Western Sahara by Morocco and Mauritania." Tradecraft Review. 2010, Special Issue, pp. 76–94, http://knbsz.gov.hu/hu/letoltes/szsz/2010_1_spec.pdf, last accessed Nov 21., 2016 and BESENYŐ, János Dárfúr a lángoló tartomány – Az Afrikai Unió szudáni missziójának története. Pécs: Publikon Kiadó, 2016; pp. 18, 23–28.

If we look at the larger context, we can realize another disturbing fact. The context in large (outside of the security policy realm) is getting more and more uncertain as well. As Friedman explained in his recent book, *Thank You for Being Late*,[16] 2007 was a watershed year for human history. Most of us have missed many upcoming disruptions. It was the year when a thing called the iPhone was introduced and based on Eric "Astro" Teller's idea (who is the CEO of Google's mysterious X research center, where he's dubbed Captain of Moonshots) technological growth has accelerated so quickly that it has now outpaced human adaptability. If this assumption is right, we are permanently behind the curve, struggling to adjust to a changing world, and better embrace uncertainty and ambiguity, because it will be the norm for the years to come. The only solution to this problem is to enhance humanity's adaptability, thus (in the case of NATO) restructuring our education and training systems, as well as the way we learn lessons must be revisited and seriously restructured very fast.
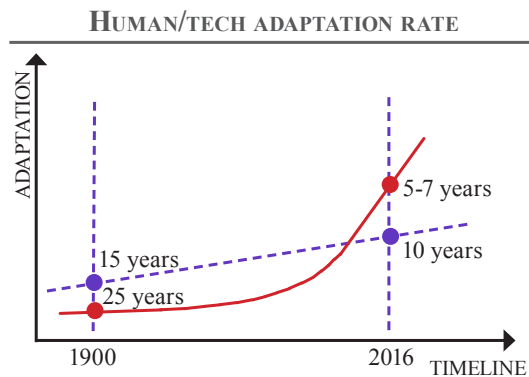
Figure 2.
The adaptation challenge[17]

The third problem in the 21st century (when constant change has become one of the most important features of our lives) is that many organizations struggle with a complex and dynamic mixture of cultures, a broad range of actors and the fact that the unprecedented proliferation of technology creates

---

16   FRIEDMAN, Thomas L. Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations. New York: Farrar Straus and Giroux, 2016.
17   The figure was inspired by Thomas Friedman: Thank You for Being Late. Friedman has published a very similar depiction of the strategic problem in his book. FRIEDMAN: Thank You for Being Late.

an ultra-competitive environment. This results in a lack of understanding, where only those, who are able to lead at the edge of chaos and able to constantly transform their organization beyond traditional means, are able to compete. Today's *complex context* creates an unsteady equilibrium where people believe that they cannot regain control and are disrupted to respond to unexpected events. Ever since the Peace of Westphalia we have experienced a period where the number of players on the battlefield was relatively constant. Thus, warfare was complicated, with moving parts, but the security environment was somewhat predictable.[18]

Most recently, however, we seem to be living in increasing turmoil, where there are no predictable outcomes, the traditional rules do not apply, the number of stakeholders in an operational theatre has increased significantly, and the interactions between these stakeholders (both ally and foe) have increased astronomically, leading to overall uncertainty and ambiguity.

The environment has shifted from complicated to complex, often described as a VUCA (Volatile, Uncertain, Complex and Ambiguous) place[19] and threats are shape-shifting much faster than it was traditionally the norm. To understand this paradigm shift, I found the *Cynefin*[20] model very useful. The model differentiates between four distinct contexts and in a nutshell, it states that simple and complicated contexts are relatively predictable, while VUCA and chaotic contexts are unpredictable, thus require a different leadership approach.[21]

Applying this model to the security environment, *simple* is a context, which is part of the history of the military at an age when the connection between input and output was right in front of you. This was the classical era, when someone could gather forces (resources), and was able to predictably calculate the effect

---

18   JOBBAGY, Zoltan: "The Social Wave-Front Analysis and the Altering Character of War: An Overview." AARMS 2011/1; pp. 197–212.

19   Things that are complex (living organisms, ecosystems, national economies) have a diverse array of connected elements that interact frequently. Being complex is different from being complicated. Things that are complicated may have many parts, but those parts are joined, one to the next, in relatively simple ways, the workings of a complicated device might be confusing, but they can ultimately be broken down and reassembled to be the same. Complexity on the other hand occurs when the number of interactions between components increases dramatically. This is where things quickly become unpredictable. MCCHRYSTAL, S. – COLLINS T. – SILVERMAN D. – FUSSELL, C. Team of teams: New Rules of Engagement for a Complex World. New York: Penguin Random House, 2015; p. 57.

20   I am using the Cynefin model by David Snowden to illustrate this. Cynefin is a Welsh word meaning haunt, habitat, acquainted, accustomed, familiar. The model is explained here in detail – http://cognitive-edge.com/, last accessed 21. Nov. 2016.

21   JOBBAGY, Zoltan: "Effects-Based Operations and the Problem of Causality: Simple and Complex," Joint Force Quarterly, 2007/3; pp. 90–95.

or the outcome of the battle. When the number of actor grew, in a *complicated* context, after the Napoleonic Era, massive armies with increasingly sophisticated equipment were fielded, and this contextual model has been perfected for generations. With the transition into the industrial age, this was the backbone of scaling large military forces and creating stable nations. This is how the military has been educated for generations: understand enough information about potential threats, analyse them, predictably budget our spending, and get a relatively good assumption to what the outcome might be. This was the mindset/mentality that we brought with us into the information age.

But the reality is that (as it was pointed out earlier) we find ourselves in a *VUCA* place for the most of the last decade. It seems that in this context our planning-based decision-making approach does not work as promised. At the same time many of the potential adversaries have adapted and developed complex systems. They don't play by the traditional rules, yet have the ability (with technology) to scale and fight. Their worldview is an environment that looks like an agile network, in contrast with the traditional systems, which lack the speed and agility that enables the organization to move/adapt like the adversaries.

Finally, in *chaos* the rule book is out the window. Disruptions are constant, and they are hitting us with increasing frequency and intensity. Our traditional approach and instinct says that we should face these situations head on, and come up with solutions, but the frequency of challenges in this state will not allow us to do this in a way that can be sustained. If we try to stick to traditional methods, they result in burnout.

Overall, regarding the contemporary context, we can conclude that there are two things driving today's change. The first one is the increase in the number of key stakeholders and the other one is interconnectedness.[22] These two forces (fuelled by technological advances in the information age and the fourth technological revolution) have resulted in an unprecedented tempo and changed the context forever. The environment has shifted from being complicated to a VUCA place[23] and as a result one can feel that threats are shape shifting much faster than it was traditionally the norm.

---

22   In population genetics this is called epistatic interactions i. e. conflicting constraints.
23   Things that are complex (living organisms, ecosystems, national economies) have a diverse array of connected elements that interact frequently. Being complex is different from being complicated. Things that are complicated may have many parts, but those parts are joined, one to the next, in relatively simple ways… the workings of a complicated device might be confusing, but they ultimately can be broken down and reassembled (to be the same)… you can predict what will happen when one part of the device is activated or altered. Complexity on the other hand oc-

Big bureaucratic organisations, like NATO, have inherited a complicated mindset, where the predominant view is that, when massive armies with increasingly sophisticated equipment are fielded, you can come up with a predictable end state. This is how the military has been educated for generations. We try to analyse potential threats, and create a plan with a relatively good assumption to what the outcome might be. It was the mindset that we brought with ourselves into the information age.

But the world is not a complicated place any longer! In an increasingly VUCA context our planning based decision-making systems and approaches do not work as promised. Many of our adversaries adapted and developed complex (networked) systems, and created an ability (supported by modern technology) to scale and fight us. At the same time, most bureaucratic organizations remained the same, what we lack is real institutional adaptation. As a result, traditional systems lack the foresight, speed and agility, as well as the reach that enables the organization to adapt like many adversaries do.

The short history of NATO's adaptation

The security environment is a fundamental driver to figure out what NATO has to do. Today's environment is determined by the *interrelation of crises*: events in one region have consequences in another region – we cannot imagine that Russia's actions in Syria are disconnected from their actions in Ukraine, for example. We also have regions facing a broad range of threats simultaneously. The Balkans, for example, face political pressure from Russia, the rise of radical Islamic groups, but also organized crime and refugee flows – and all these challenges are interrelated.

The Alliance has to realize that maybe what we were designed and optimized for is no longer applicable to today's VUCA battlefield. Complexity and uncertainty seems to be the norm of today's security landscape[24] and

---

curs when the number of interactions between components increases dramatically. This is where things quickly become unpredictable. MCCHRYSTAL et al. Team of teams. p. 57.

24 Pondy and Mitroff reminded organizational scientists 25 years ago that organizations have characteristics typical of level 8 on Boulding's 9-level scale of system complexity. Boulding concluded that organizations are among the most complex systems imaginable. BOULDING, K.E. "General Systems Theory: The skeleton of science." Management Science, 1956; pp. 2, 197–207; PONDY L.R. and MIRTOFF I. I. "Beyond open systems models fof organizations." In B.M. STAW (ed.) Research in organizational behavior. Greenwich, Conn.: JAI Press, 1979; pp. 3–39.

for an international organization like NATO with much history, legacy and past success, it is a very difficult moment. The switching approach towards strategy, which served us well in the past, in the changed security landscape does not work any longer.

Making sense of adaptation creates more confusion than clarity. It is certainly not new, and the Alliance has a long history and has undergone several focus shifts before. In fact, the Warsaw Summit acknowledged the fourth phase in NATO history. Since its creation in 1949 the Alliance first focused on collective defence. After the fall of the Berlin Wall in 1991 an era of cooperative security has started, and enlargement (especially from the former Warsaw pact countries) and the development of partnerships (including Russia) were the main focus. In 2001, after the terrorist attacks on the United States the focus shifted again towards expeditionary operations and crisis management with a strong emphasis on Afghanistan. In 2014 another focus shift started to take shape.

NATO has a high potential for adaptation and transformation, but the Alliance leadership feels that they *must choose* between tackling complex challenges or responding as a traditional bureaucratic organization and trying to survive in an age of constant disruptions (a switching strategic approach). The reality is that NATO is perfectly capable to do both at the same time. The adaptation gene in the organization (Allied Command Transformation) has the potential to contribute to NATO's overall adaptation with driving certain efforts within an integrated strategy, while Allied Command Operations can focus on the more traditional (operational) end of the spectrum. NATO's structure with the two strategic commands (and their different functions) enables the Alliance to operate and adapt at the same time. I believe that it is the only way forward in an age, when the Euro-Atlantic area is facing an unprecedented range of security challenges.

Adaptation is not new, NATO has been doing this throughout its existence,[25] but the tempo and thrust of change have changed the game recently[26] and the act of recovering from shocks is becoming almost a full-time job. Change is not an event any more, it is a process, that everyone must embrace and NATO

---

[25] NATO Secretary General Jens Stoltenberg said at the 2015 Chiefs of Transformation Conference in Norfolk, VA that "one of our greatest strengths is our ability to adapt." STOLTENBERG, Jens. Keynote speech by NATO Secretary-General at the opening of the NATO Transformation Seminar, 25. March 2015 – http://www.nato.int/cps/en/natohq/opinions_118435.htm

[26] DUNFORD, Joseph Jr. "From the Chairman: The Pace of Change." Joint Force Quarterly, 2017/1. – http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-84.aspx

is not an exception. If we look closely at what happened during the last two years, we realize that the Alliance is on the right path, but must speed up the process. In order to thrive in a VUCA[27] operating environment, when challenges are increasingly complex and interrelated and the lines between peacetime, crisis and conflict are progressively blurred, NATO needs to change mindset and develop a more networked and agile organizational structure overlaid on its traditional bureaucratic one.

The past two Summits have laid the groundwork for this journey. Three years ago at the NATO Summit in Wales in 2014, NATO leaders were clear about the security challenges on the Alliance's borders. In the East, Russia's actions threatened Europe, on the Alliance's south-eastern border, the ISIL terror campaign posed a threat. Across the Mediterranean, Libya was becoming increasingly unstable. The Alliance's leadership took decisive steps to address these challenges and reaffirmed the central mission: the shared responsibility of collective defense.[28] NATO leaders also recognized that adaptation was necessary in order to respond swiftly to emerging threats To undertake these key adaptations, NATO leaders agreed to a new Readiness Action Plan (RAP), which fundamentally changed the Alliance's posture along three interconnected and interdependent tracks.

Moreover, Allies agreed to an increase of NATO's presence in Central and Eastern Europe with additional equipment, training, exercises, and troop rotations. NATO has also undertaken a series of adaptation measures to deal with challenges in its own territory.[29] The centerpiece of this approach is

---

27 VUCA is short for volatility, uncertainty, complexity, and ambiguity. It is meant to describe the highly dynamic chaotic environment. VUCA also conflates four distinct types of challenges that demand four distinct types of responses. The notion of VUCA was introduced by the U.S. Army War College in the 1990s. The deeper meaning of each element of VUCA: (1) Volatility. The nature and dynamics of change, and the nature and speed of change forces and change catalysts. (2) Uncertainty. The lack of predictability, the prospects for surprise, and the sense of awareness and understanding of issues and events. (3) Complexity (or variety) is measured by the number of distinguishable states it is capable of having and is beyond the control of any individual. The multiplex of forces, the confounding of issues, no cause-and-effect chain and confusion that surround an organization creates and entangled web of complexity. (4) Ambiguity occurs when there is no clear interpretation of a phenomenon or set of events. It can never be eliminated altogether and the haziness of reality, the potential for misreads, and the mixed meanings of conditions always cause some confusion.

28 NATO Wales Summit Declaration – http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede240914walessummit_/sede240914walessummit_en.pdf

29 One of the most significant of these exercises was Trident Juncture 2015.

an improved and restructured NATO Response Force (NRF) that gave the Alliance a critical quick reaction capability with a high level of readiness.[30]

Following the Wales Summit, at the NATO Summit in Warsaw in July 2016, it was obvious that there are more emergent and concrete problems the Alliance has to face.[31] It seemed that NATO is being engaged in all areas of its core tasks at the same time on an everyday basis. To counter these challenges the United States quadrupled its funding for the European Reassurance Initiative (ERI) accompanied by other NATO Allies to serve as a deterrent force along NATO's eastern border.[32] There has been a pledge to strengthen individual nations' and collective cyber defences, and recognise cyberspace as a new operational domain.

It might have gone unnoticed by some, but perhaps one of the most important commitments was related to resilience, setting out areas where NATO and the EU can step up cooperation – including countering hybrid threats.[33] Resilience building is thought to be first and foremost a national responsibility, but overall the Alliance is placing a great emphasis on this topic and to find answers to the many related questions a major conference titled "Interdependency in Resilience" was organized by ACT early May 2017 in Norfolk, VA.

NATO is moving ahead, but adaptation and transformation are not easy. Preparing for the future and building strategic foresight, which enables NATO to be first to sense trouble in a complex environment (which is highly unpredictable) is becoming increasingly difficult. There are no blueprints, rules or best practices any more. Today, when security challenges demand a different kind of force, agility is essential. Thus, speed is another problem that can be addressed through increasing operational agility, and NATO's adaptation measures introduced above have partially addressed this problem. The third issue is the recognition that the root of all adaptive challenges is the same: an equilibrium of power shift

---

30   This brigade-sized spearhead force – the Very High Readiness Joint Task Force (VJTF) – enables NATO to respond more quickly. Finally, NATO shifted its posture to the east and set up eight small command and control centers (NFIUs) across the Alliance's eastern flank to serve as reception bases for either exercising forces, or – in the event of a crisis – for facilitating the reinforcement of an ally.

31   The current political and security environment created in the wake of military and humanitarian crises in Syria, massive refugee influx to Europe, DAESH's terror attacks, and the frozen conflicts in eastern Ukraine and the Caucasus, and cyber security challenges are all shape-shifting wicked-problems, which require constant transformation from the Alliance.

32   From $800 million to $3.4 billion and deploying an additional Brigade Combat Team to Europe in January 2017.

33   NATO Secretary General signed a Joint Declaration with the Presidents of the European Council and the European Commission to take partnership between NATO and the European Union to a higher level. NATO Warsaw Summit Communiqué – http://www.nato.int/cps/en/natohq/official_texts_133169.htm

towards networks. Since the number of key stakeholders in any operational setting has increased, the Alliance has to think and act like a network as well, and this requires institutional adaptation, a mindset shift followed by the implementation of a more sophisticated strategic approach.

THE LEADERSHIP PARADOX:
CHOOSING BETWEEN TWO STRATEGIC APPROACHES

When chaos hits an organization, the traditional rulebook is normally out the window. For a traditional organization, which is designed to operate in a complicated way, following a decision making process, it is necessary to make a leap from the complicated context straight into complexity. In most cases, this switch requires to shut down major components of the traditional bureaucracy while they deal with the emerging disruptive situation. If everything goes well, and a group of talented individuals engineer a solution to the problem, organizational change does not take place, they simply go back to the way it "used to be." This approach works like an on/off switch.

Leaders choosing the switching strategy[34] believe that the world can be analysed and they can foresee the future relatively predictably.[35] They tend to focus not so much on changing or shaping the environment, but rather assessing the adversaries and constructing a plan to build a sustained advantage to counter their approaches. This plan is (in most cases) executed rigorously and efficiently. The switching approach is the one that most NATO personnel are familiar with; in fact, this approach is being taught in military educational institutions and is based upon the COPD.[36] A traditional switching strategic

---

34   Architectural or structural ambidexterity, which uses dual organizational structures and strategies to differentiate efforts towards exploitation and exploration. Structural ambidexterity includes dual parts, with one part focusing on exploitation and the other focusing on exploration. ADLER P. – GOLDOFTAS B. and LEVINE, D. "Flexibility versus efficiency? A case study of model changeovers in the Toyota production system." Organization Science, 1999/1; pp. 43–68.; MCDONOUGH E. F., and LEIFER R. "Using simultaneous structures to cope with uncertainty." Academy of Management Journal, 1983/4, pp. 727–735.; TUSHMAN M. L., and O'REILLY C. A. "Ambidextrous organizations: Managing evolutionary and revolutionary change." California Management Review, 1996. summer. pp. 8–30.

35   Military thinking has always had to accommodate unpredictability, or "friction:" the divergence of reality from a plan. A leader in the past could reliably predict events further out than we can now. Monitoring and developing contingency plans to deal with fifty enemy ships is one thing; doing the same for a population of ten million people in an urban environment is practically impossible.

36   NATO Comprehensive Operations Planning Directive – https://publicintelligence.net/nato-copd/

approach typically requires short-term targets, centralization, standardization, and discipline in execution. This is exactly what NATO's Allied Command Operations does excellently and with great efficiency.[37]

The goal of the traditional approach is to build robustness and is achieved by strengthening parts of the system (the bureaucratic pyramid). It is a management approach that has been perfected throughout the last couple of hundred years and although it is highly efficient, it is not adaptable.

Since disruptions in the information age are switching constantly between complicated and complex contexts is not sustainable. If one tries to stick to traditional methods (switching back and forth) the end result in burnout, it feels like we try to stop constant waves arriving from the ocean.

The other problem in today's VUCA environment is change cycles, which (due to technological improvements and connectivity around the world) are hitting us with increasing frequency. NATO is starting to feel the state of constant disruption that pushes organizations to the edge of chaos. We realize more often that in this VUCA context traditional approaches alone do not bring about the desired result. Something else is needed to complement them.

What can we do in an age of constant disruptions? There is an alternative integrated strategy, which fuses the traditional approach with other strategic approaches and the end result is an integrated system. NATO's main challenge in this endeavour is that it has to find a way to create adaptability and agility, while preserving many of the Alliance's traditional strengths: operate and adapt at the same time. There is no manual for this transformation and we have to carry this out while facing multiple disruptions at once.

In this process NATO ultimately needs to become an integrated warfare system, and as such NATO's core principle (a network of Nations) needs to be expanded as NATO prepares for the challenges yet to come. Implementing an integrated strategy would enable the Alliance to maintain the stability and dependability of the traditional bureaucratic system, but would also layer in the right communication and decision-making functions that allow us to be as agile as the disruptive networks we are facing. Luckily, NATO has the right structure to achieve both of these goals. While Allied Command Operations is mainly focused on the traditional end of the spectrum, Allied Command Transformation has the potential to deliver a solution to build the required resilience, and agility by/with/through the member nations and NATO's many partners.

---

37   Allied Command Operations is the other NATO Strategic Command Hedquartered in Mons, Belgium.

A truly integrated strategic approach must be based on the traditional component, but additionally three other components are also necessary to make it relevant in today's VUCA context. A visionary component can sense future challenges, and identify requirements for new capabilities as well as help in fostering innovative approaches to get the latest capability innovations into the hands of the warfighter. An adaptive component would increase the speed of decision making and ensure rapid reaction. Finally, a shaping component completes the palette in a context where aligning and influencing the activities of other stakeholders (outside of the Alliance) is absolutely necessary.

The visionary component provides early warning for future challenges and more time to build capabilities to counter these challenges. Visionary leaders clearly see opportunities in places where no one else ventures. Allied Command Transformation has this built in capability and has produced the Strategic Foresight Analysis[38] as well as the Framework for Future Alliance Operations[39] documents. The recommendations have influenced NATO's defense planning process (NDPP) and as a result the Alliance is building new capabilities to counter future challenges.

The adaptive component is useful, when prediction is getting hard. Leaders using this method are more focused on adapting to change through constant experimentation, identifying new options faster than adversaries, and speeding up implementation. ACT and ACO can make sure that using lessons learned from the US third offset strategy and related NATO innovation efforts, a wide range of strategic options are generated, and tested on exercises. The most successful ones can be applied (scaled up) to form the basis of future operations. Since ACT is responsible for education and training as well as exercises, it can significantly contribute to NATO's advantage to constantly searching for innovative ideas and testing new concepts through experiments and exercises, thus making NATO a learning organization.

Finally, the shaping component is probably most important when there is an opportunity to collaborate with others in shaping (or reshaping) the security environment early on before a crisis happens (left of bang). This strategic

---

38   The 2013 SFA document can be accessed here – www.act.nato.int/images/stories/media/docli-brary/sfa_security_implications.pdf. There is also an interim update (2015) of the document which can be read here – http://www.act.nato.int/strategic-foresight-analysis-2015-report. ACT is currently working ont he 2017 SFA report.

39   The full document can be accessed here – http://www.act.nato.int/images/stories/media/docli-brary/ffao-2015.pdf

approach requires a networking mindset and an understanding that we cannot achieve our goals alone. ACT is experimenting with innovative new methods for partnering with a wide variety of stakeholders and has the capacity to build trust. This must be supported by a communication platform (a federated network) through which the Alliance can orchestrate collaboration and become part of an ecosystem. This strategic approach is very different from the previous ones since the focus here is on co-creating an entire ecosystem rather than collaboration within a single organization and amongst member nations. In fact it is so important that it will be discussed later in this paper explaining an emerging concept called the Persistent Federated Approach (PFA).

In an integrated strategy resilience is the result of linking elements that allow them to adapt in response to change and allows the system to bounce back from strategic shocks much faster with the intent for NATO to become both robust and resilient at the same time.

PERSISTENT FEDERATED APPROACH

The concept, which supports the shaping component, is the Persistent Federated Approach (PFA), which was thoroughly debated and discussed at the NATO Transformation Seminar in Budapest.[40] It supports my thesis, that although NATO has adapted before, the organisation needs a mindset shift, must revisit the functions of the command structure, and does not have the luxury of time to get it right.

The PFA concept is centered on enabling and empowering the Alliance's constituent parts to broaden the range of options. This approach requires a fundamental shift in attitude towards adaptation. NATO must make a decision between sticking to the traditional switching strategic approach, or opting for a more proactive integrated strategy.

The persistent federated approach allows multiple paths for the flow of information, and has the potential to create a shared situational awareness (better sensing and foresight) among a variety of actors. This is an approach, which would enable the Alliance to operate on a persistent basis in the VUCA context, eliminating the need for switching back and forth between

---

40   In February 2017 a Food for Thought paper was released by IISS, which was a basic starting point for the conversation at the NATO Transformation Seminar. "A Federated Way Ahead for NATO in an Age of Complexity," International Institute for Strategic Studies, Feb. 2017.

complicated and complex. It seems to be a promising alternative in a complex security landscape with benefits like increased situational awareness, improved operational agility and a networked mindset. Overall, it can lead to increased resilience, ability to project stability and also to save on resources at a time when the burden sharing question is being raised on a daily basis.

Of course there are challenges with this approach. Leading change is always difficult, and NATO needs to build this new plane as it flies (operate and adapt at the same time). The heart of the problem is an organizational transformation effort with a goal of operationalizing the new ideas and technologies and fielding new capabilities faster than our adversaries. This is what transformation is all about, and this is why ACT's function is crucial for NATO.

In the contemporary security environment those, who can get the latest technology to the warfighter faster will enjoy comparative advantage. There is a need to increase operational agility, the ability to sense, and to build a network, but it must be supported by a platform as well. This platform has to be a federated combat cloud, where the Alliance is able to build trust, create shared situational awareness with a wide range of stakeholders and share information in real time to enable almost instantaneous decision-making.

Building this platform is the goal of multiple technological solutions, but a technological fix is only one side of the coin.[41] There is a need for an organizational one as well that connects the different components of the strategy together. The present Command and Control mindset, Mission Command, as we know it, is the conduct of Military Operations through decentralized execution based on a central intent. Our need to pursue, instil and foster mission command is critical to success in today's dynamic context.[42] The basic principles of mission command (commander's intent, and decentralized execution) are not new

---

[41]   Some exampleas are the JICSPOC experiment - a horizontal integration concept in operation, which helps us better understand how to stitch all of our stakeholders together horizontally as an enterprise to better defend and create effects in and from space. "New Joint Interagency Combined Space Operations Center to be established." US DOD Press Release. Sep. 11., 2015 – http://www.defense.gov/News/News-Releases/News-Release-View/Article/616969/new-joint-interagency-combined-space-operations-center-to-be-established. Another one is the "Combat Cloud" Data to decision experiment, which aims to bridge the gap between different types of data and how that data is communicated across multiple platforms. Welsh, Patty. "Looking to a cloud to share data faster." US Air Forces Central Command, Nov. 16., 2016 – http://www.afcent.af.mil/News/tabid/4768/Article/1006428/looking-to-a-cloud-to-share-data-faster.aspx

[42]   DEMPSEY, Martin E. Mission Command White Paper. USJCS. 3. April 2012 – www.dtic.mil/doctrine/concepts/white_papers/cjcs_wp_missioncommand.pdf

concepts, but I argue that recent advances in technology make an upgrade to the concept (Mission Command 2.0) necessary.

First of all, since it is increasingly difficult to make sense of what is happening in an operational setting, experience based instinctual decision making has to be coupled with machine assisted decision making (Big Data, Deep Learning, AI). This synergistic approach which is supported by DARPA's brain research and biology efforts[43] is connecting the brain into a virtual environment, and has the possibility to revolutionize learning and decision making by improving neuroplasticity. Moreover, decisions must be communicated through a broad 'cloud based' platform, which enables the Alliance's many partners to create shared situational awareness in any given operational theatre. This continuous situational awareness; however, in the case of NATO must still be based on intent (consensus by the member Nations) and the NAC plays a crucial role here.

Mission Command 2.0 has to be the essence of the PFA. It must have the ability to concentrate, make sense of, and distribute massive amount of data. The future C4ISR architecture must be a federated one, where NATO nations and partners (states, IOs, NGOs and other relevant entities) can build a shared situational awareness, support political-military decision making, and build trust well before crisis happens.

FINAL THOUGHTS

In an age of the resurgence of state actors, and scattered protracted transnational challenges fuelled by the high-speed disruptive technological innovation, opportunities can be created even in an increasingly unpredictable context.

Since today's multiple challenges are very different, the Alliance must recognize that the most significant and capable threat to its core interests is not a resurgent and revanchist Russia, nor an Islamic State, but a systemic asymmetry between traditional bureaucratic organizations and networks. NATO leadership today faces an apparent contradiction. On one hand, austerity and intense competition pushes the Alliance to drive efficiencies (overall to survive) and

---

43   There are several projects initiated by DARPA on this field. Some are listed here: "DARPA and the Brain Initiative." DARPA, no date. http://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative.

react to multiple security challenges. On the other, the increasing pace of change pulls towards transformation (need to thrive and be more proactive).

This dilemma is not new. The Trojan horse during the Trojan War, Nelson's approach at Trafalgar, Napoleon' coup d'oeil, or the German Wermacht's blitzkrieg were major shifts in the history of warfare, transformations that no one realized and fully understood until they saw the devastating effects. NATO itself has been adapting throughout its history and we are experiencing a similar paradigm shift, which requires a different mindset, supported by a new strategic design.

In this paper I proposed an integrated strategy pointing out that implementation is both risky and painful. Only future will tell how we integrate the different strategic components, but one thing is clear: we need to think of alternative ways to fight in today's complex and chaotic battlefield.

In a VUCA context NATO needs to out-innovate adversaries. The Alliance has the potential to do this, ACT is the adaptation gene within NATO and (together with ACO and by-with-through the member states and partners) it can drive the effort for operational agility, future foresight and strategic networking. An integrated strategic approach can enable NATO to be more agile, have relatively accurate predictions, build the necessary capabilities for the future and through a network of like-minded partners, and ultimately succeed in a complex and dynamic environment.

AUTHOR'S BIOGRAPHY: Brigadier General IMRE PORKOLAB, is currently serving as NATO Supreme Allied Commander Transformation's representative to the Pentagon. His duties include aligning US and NATO ACT efforts with the Joint Staff, DoD in the Pentagon, as well as liaising with the Think Tank community in Washington DC. A Special Forces officer by trade, he has done operational tours in Iraq and Afghanistan and has served in the Hungarian Defence Forces in various command and leadership positions. He holds three masters degrees (International Relations, Military Leadership, and Defense Analysis), and has done excutive courses both at Harvard and at Stanford University. He earned his PhD in 2010. His research focus is on organizational transformation, and change leadership.

SOURCES

ADLER P. – GOLDOFTAS B. and LEVINE, D. "*Flexibility versus efficiency? A case study of model changeovers in the Toyota production system.*" Organization Science, 1999/1, 43–68.

"*A Federated Way Ahead for NATO in an Age of Complexity*" International Institute for Strategic Studies, Feb 2017.

BAKOS, Csaba Attila – FARKAS, Sándor: *Gyakorlatorientált oktatás, képzés és kiképzés, avagy a pályaszocializáció a katonai felsőoktatásban*; Honvédségi Szemle, 2016/4, pp. 85–86.

BARNO, David and BENSAHEL, Nora. "*Fighting and winning in the Grey Zone*" War on the Rocks, May 19., 2015.

BENNETT, Brian. "*NATO 'no longer obsolete,' Trump says after meeting with alliance chief,*" Los Angeles Times, Apr 12., 2017 – http://www.latimes.com/politics/washington/la-na-essential-washington-updates-despite-calling-nato-obsolete-trump-l492008895-htmlstory.html

BESENYŐ, János. "*The Occupation of Western Sahara by Morocco and Mauritania*" Tradecraft Review. 2010, Special Issue, pp. 76–94. – http://knbsz.gov.hu/hu/letoltes/szsz/2010_1_spec.pdf, last accessed Nov. 21., 2016.

BESENYŐ, János. *Dárfúr a lángoló tartomány – Az Afrikai Unió szudáni missziójának története.* Pécs: Publikon Kiadó, 2016. pp. 18., 23–28.

BOULDING K.E. "*General Systems Theory: The skeleton of science.*" Management Science, 1956, 2, 197–207

BRAGG, Belinda. "*Specifying and systematizing how we think about the Gray Zone.*" NSI, Jun. 27., 2016 – http://nsiteam.com/specifying-and-systematizing-the-gray-zone/specifying-and-systematizing-the-gray-zone/

BRANDS, H. "*Paradoxes of the Gray Zone.*" FPRI. Feb. 5., 2016 – http://www.fpri.org/articles/2016/02/paradoxes-gray-zone;

"*DARPA and the Brain Initiative.*" DARPA, no date – http://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative

DEMPSEY, Martin E. *Mission Command White Paper.* USJCS. 3. April 2012 – www.dtic.mil/doctrine/concepts/white_papers/cjcs_wp_missioncommand.pdf

DUNFORD, Joseph Jr. "*From the Chairman: The Pace of Change* " Joint Force Quarterly, 2017/1. – http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-84.aspx

ELKUS, A. "*50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense.*" War on the Rocks, Dec. 15., 2015 – http://warontherocks.com/2015/12/50-shades-of-gray-why-thegray-wars-concept-lacks-strategic-sense/;

Framework for Future Alliance Operations. Norfolk: NATO ACT, 2015 – http://www.act.nato.int/images/stories/media/doclibrary/ffao-2015.pdf

FRIEDMAN, Thomas L. *Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations.* New York: Farrar Straus and Giroux, 2016.

GARAMONE, Jim. "*Dunford Discusses Strategy, Threats at Brookings Event*" DoD News, Defense Media Activity, Feb. 23., 2017; by – https://www.defense.gov/News/Article/Article/1093155/dunford-discusses-strategy-threats-at-brookings-event/

GORKA, Sebastian and KILCULLEN, David . "*An Actor-centric Theory of War: Understanding the Difference Between COIN and Counterinsurgency* " Joint Force Quarterly, 2011/1.

GOTTEMOELLER, Rose. *Speech at the NATO Transformation Seminar*, Budapest, Hungary, Mar. 23., 2017.

Gray Zone. U.S. Special Operations Command White Paper. Tampa: USSOCOM, Sep. 9., 2015.

JOBBAGY, Zoltan: "*Effects-Based Operations and the Age of Complexity: A Critical Reflection*" Militaire Spectator, May 2006; pp. 235–242.

JOBBAGY, Zoltan: "*Effects-Based Operations and the Problem of Causality: Simple and Complex*" Joint Force Quarterly, 2007/3; pp. 90–95.

JOBBAGY, Zoltan: "*The Social Wave-Front Analysis and the Altering Character of War: An Overview*" AARMS 2011/1; pp. 197–212.

KRULAK, V. (1984). *First to Fight: An Inside View of the U.S. Marine Corps.* Annapolis: Naval Institute Press, Ch12.

MATTIS, Jim. "*Remarks by Secretary Mattis at the Munich Security Conference in Munich, Germany*" US DoD, Secretary of Defense Speech, Feb. 17., 2017 – https://www.defense.gov/News/Speeches/Speech-View/Article/1087838/remarks-by-secretary-mattis-at-the-munich-security-conference-in-munich-germany/

MAZARR, M. J. *Mastering the gray zone: understanding a changing era of conflict.* Carlisle: Strategic Studies Institute, Army War College Press, 2015 – http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1303.

MCCHRYSTAL, S. – COLLINS T. – SILVERMAN D. – FUSSELL, C. *Team of teams: New Rules of Engagement for a Complex World*. New York: Penguin Random House, 2015; 57.

MCDONOUGH E. F., and LEIFER R. "*Using simultaneous structures to cope with uncertainty*" Academy of Management Journal, 1983/4; pp. 727–735.

NATO Comprehensive Operations Planning Directive – https://publicintelligence.net/nato-copd/

NATO Wales Summit Declaration – http://www.europarl.europa.eu/
meetdocs/2014_2019/documents/sede/dv/sede240914walessummit_/
sede240914walessummit_en.pdf

NATO Warsaw Summit Communiqué –http://www.nato.int/cps/en/natohq/official_
texts_133169.htm

"New Joint Interagency Combined Space Operations Center to be established."
US DOD Press Release. Sep. 11., 2015 – http://www.defense.gov/News/News-
Releases/News-Release-View/Article/616969/new-joint-interagency-combined-
space-operations-center-to-be-established

"*Not at Peace and Not at War: An Exploration of 'Gray Conflicts'.*" Joint Strategy
Review Study. 2015.

Outplayed: Regaining the initiative in the Grey Zone. (Nathan Freier, project director)
Carlisle Barracks: Strategic Studies Institute, United States Army War College
Press, 2016.

PELLERIN, Cheryl. "*Mattis: NATO is Evolving in Response to New Strategic
Reality*" DoD News, Defense Media Activity. Feb. 16., 2017 – https://www.
defense.gov/News/Article/Article/1085796/mattis-nato-is-evolving-in-response-
to-new-strategic-reality/

PONDY L.R. and MIRTOFF I. I. "*Beyond open systems models fof organizations*"
In B.M. Staw (ed.) Research in organizational behavior. Greenwich, Conn.: JAI
Press, 1979; pp. 3–39.

STOLTENBERG, Jens. K*eynote speech by NATO Secretary-General at the opening
of the NATO Transformation Seminar,* 25. March 2015 – http://www.nato.int/
cps/en/natohq/opinions_118435.htm

Strategic Foresight Analysis 2013 Report. Norfolk: NATO ACT, 2013 – www.act.
nato.int/images/stories/media/doclibrary/sfa_security_implications.pdf.

Strategic Foresight Analysis 2015 Update Report. Norfolk: NATO ACT, 2015 – http://
www.act.nato.int/strategic-foresight-analysis-2015-report.

TUSHMAN M. L., and O'REILLY C. A. "*Ambidextrous organizations: Managing
evolutionary and revolutionary change*" California Management Review, 1996.
summer. 8–30.

VOTEL, Joseph L. – CLEVELAND, Charles T. – CONNETT, Charles T. and
IRWIN, Will. "*Unconventional Warfare in the Gray Zone*" Joint Forces
Quarterly, 2016/1.

WELSH, Patty. "*Looking to a cloud to share data faster*" US Air Forces Central
Command, Nov. 16., 2016 – http://www.afcent.af.mil/News/tabid/4768/
Article/1006428/looking-to-a-cloud-to-share-data-faster.aspx

ROMULUSZ RUSZIN
Are the Current Principles
of War Still Applicable?

Moreover such instances pave and prepare the way for the operative part, as will be shown in the proper place, when I come to speak of deductions leading to Practice. [1] FRANCIS BACON

ABSTRACT: Today's armies are largely influenced by the ideas that emerged from the Napoleonic era, and rely on fundamental principles of war that are the product of experience gained in the Second World War. However, armed conflict in the 21st century has become more complex due to the wide range of participants and the increased numbers of warfighting domains. Time, collective experience and the significantly changed circumstances suggest that the principles of war be reformulated. The paper recommends reducing the number of principles to a manageable handful, and offers five new Principles of War which should always be used jointly to reach the desired end-state successfully at every level, in every domain, and by every participant.

INTRODUCTION

The art of war and the principles of armed conflict have been pondered across the millennia. In every age, theoreticians seemingly have arisen to declare what principles to apply to win war. However, today's armies are significantly influenced by the ideas that emerged from the Napoleonic era. One of these theorists, Antoine-Henri Jomini, went as far as to suggest a near scientific approach to war.[2] Jomini and others with a similar line of thought assert that there are specific principles that one needs to apply, in order to prevail in battle. They have written a great many words on clean white sheets of paper to teach

---

1   BACON, Francis. The New Organon, Book II. in The Works of Francis Bacon vol. iv. Cambridge: Cambridge University Press, 2011; page 173.
2   JOMINI, Antoine-Henri. The Art of War. Novato, CA: Presidio Press, 1992.

---

their ideas to subordinates, colleagues and even to the political leadership on how to win war "scientifically" or "mathematically."[3]

In addition to the scores of ideas expounded by theorists, armies and alliances have also published numerous documents (doctrines, manuals, handbooks, STANAGs and other tactical, operational and strategic publications) to explain how it is possible to win wars. Nearly all of these theories or concepts begin with principles of war – the attributes of armed conflict that theorists say are essential to winning. These principles include everything from the value of unity of command, through surprise, to the concept of maneuver. The professional soldier (officer, NCO and enlisted) has literally dozens of principles to study and apply when thinking about war.[4]

The main question is whether such a litany of principles is still useful, or perhaps the nature of armed conflict has changed sufficiently for us to reconsider the ideas mainly rooted in the Napoleonic era. Perhaps this should be approached in another manner; ascertaining if it is possible to create a new "short list" of principles which is applicable in every type of armed conflict from a fight between two men to all-out war?

This essay will analyze the different circumstances and characteristics of armed conflict to ascertain if the existing principles of war are relevant. After that, a short list of the essential principles of war will be provided to initiate a debate on how to resolve this dilemma. Finally, to focus the argument, a discussion

---

3   Most of the current principles are based on one of the great theoreticians' publication from various ages and cultures. For instance, books published by Sun-Tzu, Jomini, Clausewitz consist of several principles such as offensive, mass, security, morale etc, which are still part of the list of principles of war in various publications.

4   Some example to support the statement: There are more than 300 Field Manuals which is only one type of doctrinal publication in the US military, http://armypubs.army.mil/doctrine/Active_ FM.html, Accessed: October 14., 2013; there is currently 123 publicly available NATO STANAGs – http://nsa.nato.int/nsa/nsdd/listpromulg.html, accessed: October 14., 2013 and there are more which are not openly available. Every nation has its own tactical, operational and strategic official publications. Some examples of fundamentals or principles beside principles of war: Doctrine for the Armed Forces of the United States, Joint Publication 1, 25. March 2013, V–1, VI–1 has general principles in the Chapter V and other principles in Chapter VI.; Ranger Handbook United States Army, Ranger Training Brigade United States Army Infantry School, Fort Benning, Georgia, April 2000, pages 1–1, 1–2 introduce 13 principles of leadership; FM 90–26 Airborne Operations Washington DC: Headquarters, Department of the Army, December 1990, page 1–5 highlight the fundamentals of Airborne Operations; Peace Support Operations AJP–3.4.1, North Atlantic Treaty Organization Standardization Agency, July 2001, pages 3–1 – 3–6 has an entire chapter on the fundamentals of Peace Support Operations; Manual of NATO safety principles for the storage of military ammunition and explosives AASTP–1, North Atlantic Treaty Organization Standardization Agency, May 2010 deals with principles on 588 pages.

follows on the military aspect of war, without touching on the other instruments of national power.

Principles of War

Principles of war are the practical implementation of the theory of war.[5] Most nations view them as the key to winning battles, and ultimately war. To be sure, the principles of war are based upon historic study of armed conflict across the millennia. As such, they tend to be enduring truths that have made the difference in how an armed force attained victory.

Military forces can participate in diverse types of conflict. Figure 1. shows the various characteristics of military operations that a military force may have to engage in. It should be noted, however, that Figure 1. does not include every operational category or sub-category. For example, Peace Support Operations can be divided into such sub-categories as peace building, peacekeeping, peace enforcement, peacemaking, and conflict prevention.[6] And since the very nature of operations is that they are dynamic, it should be obvious that one type of armed conflict can morph into another type conflict.[7]

---

5   This statement is the author's understanding of principles. Studying Sun Tzu's five fundamentals and seven elements, Clausewitz's overall principles in his primary work, as well as current tactical and operational publications has convinced the author that the principles of war summarize the characteristics of successful operations. SUN TZU. The Art of War. New York: Oxford University Press, 1963, 63. CLAUSEWITZ, Carl von. On War. Princeton, NJ: Princeton University Press, 1976. Army Field Manual, FM-3 Military Operations. Washington DC: Headquarters, Department Of The Army, 27. February 2008; A-1.
6   *Peace Support Operations AJP–3.4.1.* Chapter 2.
7   Historical evidence in Iraq and in Afghanistan where after the declaration of end of war, military forces started to conduct stability operations which eventually turned into counterinsurgency operations.
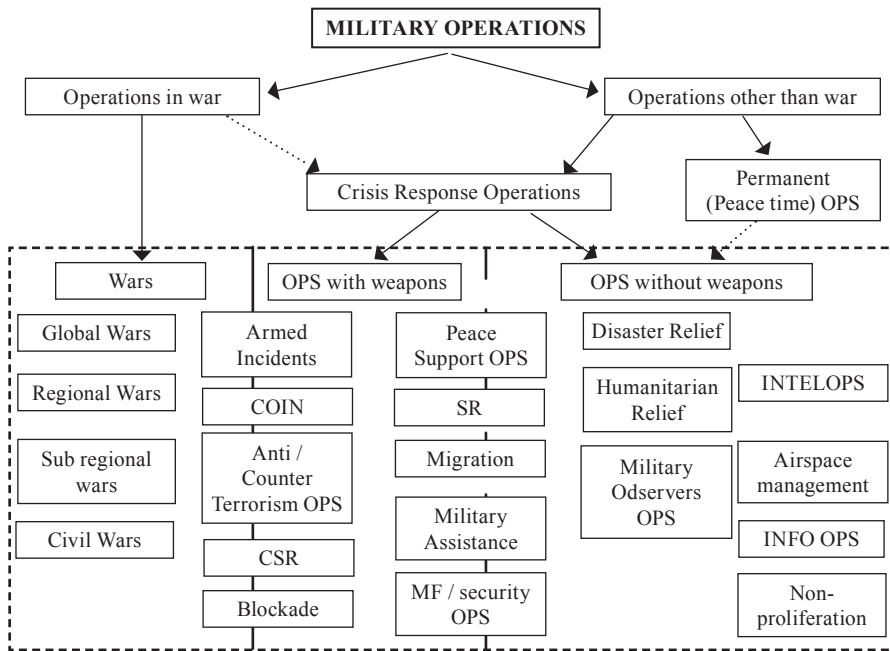
MILITARY OPERATIONS

Operations in war

Operations other than war

Crisis Response Operations

Permanent (Peace time) OPS

Wars

OPS with weapons

OPS without weapons

Global Wars

Armed Incidents

Peace Support OPS

Disaster Relief

Regional Wars

COIN

SR

Humanitarian Relief

INTELOPS

Sub regional wars

Anti / Counter Terrorism OPS

Migration

Military Odservers OPS

Airspace management

Civil Wars

CSR

Military Assistance

INFO OPS

Blockade

MF / security OPS

Non-proliferation

Figure 1.
Possible Military Operations[8]

Understanding the complexity and diversity of conflict as portrayed in Figure 1, a military force may find itself applying outdated Napoleonic principles of war.[9] This is particularly dangerous when military and political leaders view the principles of war as a silver bullet. Such a view of armed conflict creates a dilemma

---

8   The Figure was created by the Author based on: DEÁK, János. "Napjaink és a jövő háborúja" (Current and future war), Hadtudomány, 2005/1. 29–49.; The Charter of the United Nations. New York: UN Publications [http://www.un.org/en/documents/charter/] accessed May 29., 2013; Allied Joint Doctrine, AJP–01(D), North Atlantic Treaty Organization Standardization Agency, December 2010; Peace Support operations AJP–3.4.1.; Strategic Concept (SC 99/ MC 327/2 (Final), NATO Military Policy for Non-Article 5 CRO, 29 Aug 01; NATO Glossary of terms and definitions (English and French) AAP–06, North Atlantic Treaty Organization Standardiza-tion Agency, 2013; The Author's PhD essay: RUSZIN Romulusz. A Magyar Honvédség Tábori Tüzérségének alkalmazási lehetőségei béketámogató műveletek során. (Opportunities for the employment of the field artillery of the Hungarian Defence Force in Peace Support Operations). Zrínyi Miklós National Defense University, Hungary 2009 – http://portal.zmne.hu/download/ konyvtar/digitgy/phd/2010/ruszin_romulusz.pdf, accessed October 07., 2013.
9   For example the US Army has had the same principles since 1949, ETTRICH, Brian B. *The Principles of War: Are they still applicable?* Naval Postgraduate School, Monterey, California, Thesis, June 2005 calhoun.nps.edu/bitstream/handle/10945/10011/05Jun_Ettrich.pdf?sequence=1 accessed 07/10/2013; page 78.

for planners who are hard pressed to develop a plan that both fits the politician's expectations while at the same time abiding by the time-proven ideals embodied by the principles of war. The challenge is applying a "text-book" understanding of the principles of war in contravention to the realities of what is actually happening "on the ground." It is daunting, and often even impossible to predict what the enemy will do, how he will fight and where and when he will strike.

Another problem is that although many planners may know the terminology related to the principles of war, they may not actually know what they mean. It is a common occurrence of hearing planners speaking about center of gravity, when they are actually describing a decisive point or critical capability.[10] To quote Alexander Pope, *"a little knowledge is a dangerous thing."*[11] And then there is the problem that most nations have of their own principles of war, meaning that many armies do not approach or understand war in the same context.

Table 1. details a study of 14 nations' and NATO's Principles of War conducted by the author.12 This includes thirty-six different principles of war – although in some cases different names may refer to the same thing (e.g. Objective and Selection and Maintenance of Aim, or Surprise and Trick). Looking at it closer, most states have between nine and twelve principles, except France, which has only three. It seems that the nations with a longer list of principles are attempting to cover every contingency, and that instead of having a useful short list of essential concepts, they rather encompass the gamut of armed conflict.

10　This is the Author's experience based on several deployments and training exercises in multinational environments in Iraq, Afghanistan, Germany, Italy and Hungary. For the US view on center of gravity and decisive point see: Joint Operation Planning. Washington DC: Joint Publication 5-0, August 11, 2011 Page III–22–26.

11　POPE, Alexander. *An Essay on Criticism*, 1709, http://www.phrases.org.uk/meanings/a-little-knowledge-is-a-dangerous-thing.html, Accessed: December 10., 2013.

12　The table is the result of research by the author while studying at the US Army War College, Academic Year 14. Sources for establishing the table: Allied Joint Doctrine for The Conduct of Operations, AJP–3(B). NATO Standardization Agency, March 2011, Page 1–6.; Military Operations FM–3. Washington DC: Headquarters, Department of the Army, 27. February 2008, Appendix A, A1–A4; Joint Doctrine Publication 0–01: UK Defence Doctrine, Fourth edition, London: Ministry of Defence, 2011, Page 2–3.; Canada's Army, B-gl-300-000 Fp-000 (Cfp 300) Canada's Army, Caf, 2001 – http://www.scribd.com/doc/98779561/B-gl-300-000-Fp-000-Cfp-300-Canada-s-Army-Caf-2001, accessed 22/10/2013; Campaign Manual C100–5 – Operations, 3rd Edition, Brasília, Federal District 1997, The Army (Revised Edition), Army Manual M 1 TD, The Malaysian Army/Armed Forces, 2010; Land Doctrine Publication, Military doctrine for land operations, Netherlands Operation Training Centre, 2009, 6293; "Principles of war in the Soviet Union and Russia" – http://dictionary.sensagent.com/principles%20of%20war/en-en/ - 30/06/2013; MALLICK, P.K. Principles of War: Time for Relook, The Centre for Land Warfare Studies, New Delhi, 2009, Appendix A; as well as the Author's research using the National Principles of War Interpreted by International Fellows AY14 of USAWC.

The rule of 7 ± 2 is applicable here because the principles must be known to always be effective.[13] That is, the principles have to be part of the critical and creative thinking of staffs and commanders to help them determine the best plan to win.[14] However, it seems that fewer is better in the case of the principles of war, as it will make it easier for the same staffs and commanders to develop a cogent plan during planning and execution phases of an operation.[15]

Table 1.
Comparison of Principles of War of Various Nations

Principles	USA	Great Britain	Canada	Australia	India	Israel	Former USSR	France	China	Japan	Saud Arabia, Brazil	Malaysia	Netherlands	NATO19F[16]	SUM
Objective	x					x[17]				x	x			x	5
Offensive (Action)	x	x	x	x	x	x	x[18]		x		x	x			10
Mass	x						x			x	x				4
Economy of Force	x			x			x				x				5
Maneuver	x									x	x				3
Unity of Command	x										x				2
Security	x	x	x	x	x	x	x		x	x	x	x	x	x	13
Surprise	x	x	x		x		x	x	x	x	x	x	x	x	12

---

13 This Author agrees with the view that the human mind is able to concentrate on maximum 7 ± 2 different directions at the same time for longer period. This is the basis of graphology, among other things; moreover, this is the main guidance of organizational building as well. For additional background see KNAUSZ Imre, A tanítás mestersége (The profession of teaching) – http://mek.niif.hu/01800/01817/01817.htm, accessed October 07., 2013.

14 For additional background see: HALPERN, Diane F. "Creative Thinking," in Thought and Knowledge: An Introduction to Critical Thinking, 4th ed. Mahwah, NJ: Lawrence Erlbaum Associates, 2002, 396–417 and 426–429. and GERRAS, Stephen J. "Thinking Critically about Critical Thinking: A Fundamental Guide for Strategic Leaders," in Planner's Handbook for Operations Design, Version 1.0. Suffolk, VA: Joint Staff, J–7, October 7., 2011; C–1 – C–27.

15 "Principle is a general or fundamental truth; a comprehensive and fundamental law, doctrine, or assumption on with others are based or from which others are derived; natural law or laws applied to achieve a purpose or produce a result by an artificial device (as a mechanical-contrivance)", Webster's Third New International Dictionary of the English Language Unabridged, G&C Merrian Company, Springfield, Massachusetts, USA, 1961, page 1803.

16 Most of the NATO members ratified the NATO STANAG's principles into national doctrine.

17 Israel uses: tenacity due to the objective.

18 Former USSR doctrine used simultaneous attack in depth.

Principles	USA	Great Britain	Canada	Australia	India	Israel	Former USSR	France	China	Japan	Saudi Arabia, Brazil	Malaysia	Netherlands	NATO19F[16]	SUM
Simplicity	x					x				x	x		x	x	6
Selection and Maintenance of Aim		x	x	x	x				x			x	x		7
Concentration of Force		x	x		x	x			x			x	x	x	8
Flexibility		x	x	x	x	x			x			x	x	x	9
Cooperation		x	x	x	x							x			5
Morale (Maintenance of Morale)		x	x	x	x		x		x			x	x	x	9
Administration			x		x							x			3
Concentration of Effort				x		x		x							3
Economy of Effort		x	x	x								x		x	4
Sustainability Sustainment		x		x									x	x	4
Extraction of Force						x									1
Initiative						x	x		x	x			x	x	6
Trick						x									1
Continuity						x									1
Depth and Reserve						x									1
Fighting Spirit						x									1
Liberty (Freedom) of Action								x	x						2
Mobility									x						1
Coordination							x		x						2
Political Mobilization							x		x						2
Caution										x					1
Unity of Effort										x			x	x	3
Mobility and tempo							x								1
High Combat Readiness							x								1
Multinationality														x	1
Freedom of movement													x		1
Legitimacy													x		1

The most commonly cited principles are: security, surprise, offensive, flexibility, and morale. A starting point in this discussion may be to focus on these five principles as being the key, with perhaps one or two others added in

for good measure.[19] Yet, such an approach may not be enough. I suggest that by using simple terms with well-established definitions categorized by their central theme it will be possible to reduce the number of principles. With that framework in mind, the following five key elements of armed conflict can be discerned in table 1.:

1. Never initiate action without distinct advantages.
2. Always maintain communication with friendly forces.
3. Always respect opposing forces.
4. Never lose sight of your objective.
5. Build and use a clear chain of command.

Of course, due to the various possibilities of armed conflicts and the diversity of circumstances, there are more fundamentals which can help in war. Yet, the intent of this paper is to view the principles of war in a less complicated manner.

Principle 1:
Never initiate action without distinct advantages

This is arguably the most important principle, because it forces the participants to ascertain their end state before going to war. If during contemplation of this principle it is determined that it is unlikely to defeat the adversary, then the planners would press the decision makers to avoid direct conflict.[20] This does not mean that the main goal must be given up, but it is better to delay kinetic actions until an advantage can be secured over the adversary.

This principle can answer the HOW question as well. This is of key importance, because it helps planners to contemplate the other principles. The importance of this principle is enhanced, since war now extends beyond the traditional three domains of air, land and sea, but also now encompasses, space and cyberspace as well.[21]

---

19   The Author agrees with the thesis summary of ETTRICH. *The Principles of War.*
20   This theory – indirect warfare – was explained by Clausewitz as well. For additional background see: PERJÉS, Géza. *Clausewitz*, Budapest, Magvető, 1983.
21   For additional background see: BROWN, Gary D. and TULLOS, Owen W. *On the Spectrum of Cyberspace Operations*, Small Wars Journal, 11. December 2012 – http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations, accessed: December 08., 2013 and NORTH, Gary L. and RIORDAN, John. *The Role of Space in Military Operations: Integrating and Synchronizing Space in Today's Fight,* High Frontier 4, no. 2. February 2008; pp. 3–7. –

Facing this complex and diverse battlespace is the commander, who has the responsibility to evaluate his organization's strengths and weaknesses and with that in mind, deploy his forces in the best manner to gain an advantage over his foe. It was difficult even without the two newly introduced domains. It is not easy to analyze everything, and basically the hardest part of staff work is to produce enough accurate information to the commander to make the right decisions. It is a multi-faceted analysis, which is never finished, and continuously touches the current situation and the opportunities of friendly and enemy forces.[22] But this is essential before issuing orders to start the next action.

This is the responsibility of the commander at every level. It doesn't mean that he has the option to refuse the execution of his orders because according to the analysis of his staff victory seems to be impossible. Rather, every commander has to be capable of identifying opportunities for his forces to create enough advantage to win.

Summary of the first principle:
- Numbers.
- Equipment.
- Techniques, Tactics and Procedures (TTPs):
  - choose the right type of warfare;
  - balance between various types of maneuver, position and fires;
  - power of surprise, strength, aggressiveness, speed;
  - seizing and retqining the initiative;
  - flexibility in time, place and forces employed;
  - advantages of knowing and using the restrictions and opportunities of terrain;
  - effective outcomes of deception.
- Human factor.
- Using resources and every domain such as land, air, sea, space, and cyberspace.

http://www.afspc.af.mil/shared/media/document/AFD-080226-050.pdf accessed December 08, 2013; *Joint Operation Planning.* Page III–1–5.

22   For additional background see: *Joint Operation Planning.* Page III–1–5.

PRINCIPLE 2:
ALWAYS MAINTAIN COMMUNICATION WITH FRIENDLY FORCES

The essence of this principle is to know at all times where own troops are, and what their current activity is, so that their fire and maneuver can be leveraged in the right place, at the right time. The importance, as a principle, of different types of leadership and command and control systems will be explained by the 5th principle. Applying this principle creates a workable foundation, so that the commander (or the political leader) will be able to give orders to the units, guidance to the staff, and understandable policy to the non-military and sometimes non-governmental organizations.

This principle is necessary at each level of leadership in all conflicts, from squad leader through army general and prime minister to commander of an alliance's forces and chairman of the main committee of an alliance, in order to develop, deliver, and sustain the leadership messages.[23] It has never been enough to obtain a clear picture of a situation but it has been essential to transfer it to the higher command without any distortions. The real time and authentic mission analysis, which is based on the current situation, manages to give a chance to the leadership to take and keep the initiative.

The main challenge of the planning process at all levels is time. Time, because if we take a look at the time line we have to realize that the decision is made at the end of the first third of the planning and preparation phase. It is necessary to give adequate time to the subordinates so that they can prepare themselves for execution. However, during the rest of the time, which is twice as much as used for making the final decision, staff and units receive (if the communication is in tune) thousands of pieces of information which can affect the execution. (Figure 2)

---

23   For additional background see: BALDONI, John. *Great Communication Secrets of Great Leaders.* New York: McGraw Hill, 2003.
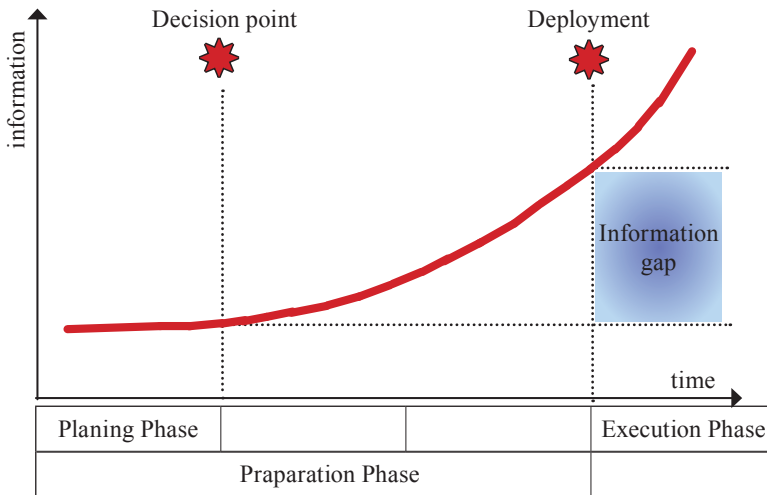
Figure 2.
Challenge of the relations of the time and information [24]

This problem increases during battle, because the situation is changing very fast and therefore the communication is essential so that commanders will be capable of adapting to the already changed situation. To foolishly stick to the plan without adapting it to the realities of the developing situation has caused nations to lose wars.

Now, go back to the idea of time as an important factor for staffs to have enough of it. As Napoleon said, *"You can ask me for anything you like, except time."*[25] This relation to time is significant throughout an organization, and one factor – the adequacy of communications – can have a disproportionate impact. Even with today's advanced technologies, communications can eat up a lot of the available time. The information about current and upcoming operations is vital for the higher command and for the subordinates (the vertical information sharing chain), but it is at least as important laterally, for the neighboring units and other friendly forces, as well as civilian participants. As the tempo and complexity of operations increase, the traditional communication channels usually prove inadequate for the task: they are too slow, and may not reach crucially important partners. In addition, a lot of time

---

24   The Figure was created by the author based on the presentation of LTC Sándor Kósa in the Hungarian National Defense University MsC lecture, Budapest, 2002.
25   http://www.napoleon-series.org/research/napoleon/c_quotes.html, accessed: December 08., 2013

may be wasted in "handshaking" – the repeated coordination with agencies that are new, unexpected, or temporary partners in an operation. This clogs up the communications channels, causes delays, and may lead to the failure of even the best-conceived operation, due to delays in execution or poor timing. It is critical to be successful in this area, because only well-coordinated common actions, based on timely information, can achieve maximum success with minimum damage. In addition, with perfect and live communication it is possible to reduce the possibility of "friendly" and "Green-on-Blue" Fires. Real-time communication became important during crisis situations, even between adversaries.

Workable communication has two main parts. The first is the technical side which must provide equipment for sending and receiving understandable real time information. The second is the well-known and unmistakable language of the message. At the beginning of the 21st century some people only believe in communication systems provided by cutting age technology. They are, of course, right in most situations because developed communication systems based on satellite and frequency-hopping can create advantages according to the first principle.[26] However, it is a kind of race, similar to the one between armored vehicles and anti-tank weapons, or between multipurpose jets and air-defense systems, because communication systems and electronic warfare solutions and listening stations are eager to understand the opposite side's communication and try to jam it.

Besides this well designed capacity, the traditional ways of communication are still useful. Different hand signs, body-language, eye contact, flag signals, and code words are still essential especially at the tactical level. Furthermore, it is pretty hard to jam them.

There is one more significant segment of the technical side of communication. Each type of technical solution has to be capable of providing a two-way transmission. One-way is better than nothing, but practical communication needs both sides' participation, because only this type of conversation can build real communication and interaction. Feedback, situation reports, early warning reports or even of the request for MEDEVAC, CASEVAC (Medical Evacuation, Casualty Evacuation) are essential for both sides, therefore, sending a message most of the time is not enough.

---

26   There are many examples when communication based on cutting-edge technology gave not only tactical advantage but also saved lives due to the possibility of calling for MEDEVAC and CASE-VAC anywhere, any time, either in Iraq or in Afghanistan.

And this is the place where the language of communication becomes essential especially in an international environment, because *"the task of training, advising, and partnering with foreign military and security forces has moved from the periphery to become a critical skill set across our armed forces"*.[27] Nations have been sending their units to war for ages. The community of international soldiers has extensive experience in multinational cooperation not only during training but also in armed conflict. *"The first two peacekeeping operations deployed by the UN were the UN Truce Supervision Organization (UNTSO) and the UN Military Observer Group in India and Pakistan (UNMOGIP)"* from May 1948.[28] Here the importance of training must be highlighted. It is crucial for every defense force that intends to, or is constrained to take part in an armed conflict directly.[29] Furthermore, joint task forces, that include a Coalition of nations have, over the years learned that it is not enough to synchronize their procedures, but they need to understand each other as well. To do it in a proper way, they must use the same language with almost the same dialect.

Using a common language is essential as a minimum basic requirement in the case of a mixed nationality operation. However, it is almost impossible to create an international task force where everybody has fluency in a common language. Finding positions and assignments where a certain level of language capability is dictated is necessary before operation commence. To make it simple, the best solution seems to be if the commanders (from a fire team to the supreme command of an alliance), the members of the staff at each level, and of course every soldier serving in communications billets have a universal communication potential. It has worked and it will work as well, and in addition it helps to create the organization chart before the establishment of a joint task force. Therefore, it is always more fruitful if nationality based compact units and organizations are put together because the native command language helps to avoid receiving and giving misunderstand-able commands and reports.

---

27   PANETTA, Leon E. *"Building Partnership in the 21st Century,"* Dean Acheson Lecture, US Institute of Peace, 28. Jun. 2012, page 2

28   "The early years: UN Peacekeeping was born at a time when Cold War rivalries frequently paralyzed the Security Council United Nations official home page, peacekeeping operations." United Nations official home page – http://www.un.org/en/peacekeeping/operations/early.shtml, accessed: December 08., 2013.

29   "There are no secrets to success. It is the result of preparation, hard work, and learning from failure." Attributed to Colin Powell. It is a living warning sentence. It is true at the national and international level because soldiers need to practice, moreover need to put into the muscle memory every possible procedure.

Although a common language is vital, it is not enough. Different languages have different vocabularies with different meanings which are sometimes very similar to each other. For example the two tactical tasks (block and fix) have different aims therefore the execution must be different if a unit receives one of these tasks, but in the Hungarian language they have the same meaning. The meaning of these (and of course several other) tactical tasks are described in official publications such as FM 100-5, AAP-6, Commander's Handbook and these are already translated and explained in the Hungarian language as well.[30] If the participants are not aware of the precise meaning of these terms they can easily misunderstand the order and waste too much time or in a worst case scenario they may cause the whole mission to fail.

Common language means knowing our partner's culture as well. Recent and possible future conflict resolution demands effective interagency collaboration. Different nations' armed forces, own services and branches, governmental and non-governmental organizations, state and non-state actors had, have, and will have significant role in armed conflicts therefore the cooperation and coordination are not avoidable segment. The following quote from Brent Scowcroft highlights this dilemma;

> "*There is no place on earth that cannot become tomorrow's crisis. Globalization is eroding borders and individual states' abilities to manage transnational challenges... they demand the use of more than simply military force or traditional diplomacy. In many cases, problems will require the use of all forms of U.S. power and influence, be it hard military or economic power, persuasive diplomacy, development aid for nation building, or soft power to attract nations and people toward seeing the world more like we do. This requires an extraordinary degree of coordination of these instruments across the entire U.S. government."[31]*

The "common language" is responsible for providing common understanding concerning values, interest, aim and objective at every level among participants internally and externally as well. They must respect each other and must respect other organization's capability and interest without losing the 4th principle.

---

30   KÓSA, Sándor and RUSZIN, Romulusz. *A harcászati feladatok osztályozása és tartalmuk meghatározása, (Types and definitions of tactical tasks)* Budapest, Hadtudomány 2005/3 42–48.

31   SCOWCROFT, Brent. Foreword to: GEORGE, Roger Z. and RISHIKOF, Harvey (eds.) *The National Security Enterprise: Navigating the Labyrinth.* Washington DC: Georgetown University Press, 2011. xi–xii.

Summary of the second principle:
- To know where our troops exactly are.
- The challenge of time.
- Lateral and vertical communication.
- Technical segment of communication.
- Common language in communication.
- Understanding of definitions, organizational and professional culture.

Principle 3:
Always respect opposing forces

If there is one thing that history has demonstrated it is that it is foolhardy to under-estimate your adversary.
- Perhaps their forces seemed inadequate, or their equipment archaic; either way one must always respect the enemy lest one be caught unawares. Observing the principle of respecting your foe keeps the military instrument of power vigilant against being surprised or caught off guard. This tenet is important especially during conflicts when battles and kinetic contact flow continuously. In addition, the respect of the opposite forces helps avoid unreasonable self-confidence which has caused sudden defeat.
- Contemporary conflicts call for the capacity for continuous analysis of the enemy at the tactical, operational and strategic levels of war. One of the most important parts of this analysis is to have as clear a picture of the belligerents as possible. *"The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to 'connect the dots.' No one component holds all the relevant information."*[32] It means, we must know and compare the forces arrayed in battle, both friend and enemy. It is a non-stop activity because the possibility of rapid change, and in particular change in the conditions that influence the first principle is obvious. Also, both sides use the outcome of the last conflict's lessons learned and try to shape their combat effectiveness to be successful.
- The personality and character of the commander is a decisive piece of the action of forces, therefore it deserves special attention, because it helps to figure out how to change the behavior of the forces in the the-

---

32   *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-01 Washington, DC: US Joint Chiefs of Staff, 05 January 2012, page II–1

atre. Measuring actions and interactions of the leaders, studying their education history, and examining their former experiences, including their decision making process, can shape their possible future activity. It is important not only in the enemy's case, but also good to know the subordinates and partners capability especially in joint and international environment.

● It is not enough to know and share information but necessary to use and interpret it to shape future activities. Also, we must not forget that we are measured by the enemy as well; therefore to be unpredictable is the essence of success and not just the basic fundamental of survival.

● Developing a new weapon system or transforming the organizational structure of one's forces is mainly a mid- to long term adaptation. Shaping and varying the operational and tactical procedures or even the strategic answer is easier in short term. With this in mind the type and frequency of change depends on the characteristic and the level of conflicts but the most important is to not forget its necessity. The change is effective if friendly forces will not be surprised and the enemy ends up in an unpredictable situation.

● This fundamental leads us to the importance of Operational Security (OPSEC). The "WikiLeaks scandal" provides ample evidence about its importance.[33] Every member of the national instruments has a responsibility to pay special attention to safeguard classified information. Leadership's duty is to implement active and passive measures and bureaucratic policies inside the organization to keep OPSEC high. The challenge is how it is possible to share essential dates and information in interagency and international operation among military services, branches, governmental and non-governmental organizations without leaking anything.

Summary of the third principle:
● Good to know:
  ▪ Enemy's capability, strength, weaknesses.
  ▪ Capability, strength and weaknesses of friendly forces.
  ▪ Characteristics of the enemy's commander.

---

33   For additional background see: FUNARO, Kaitlin. *WikiLeaks scandal's Bradley Manning: 'I'm going to die' in military prison,* http://www.globalpost.com/dispatch/news/regions/americas/united-states/121129/wikileaks-bradley-manning-im-going-die-military-, Accessed: December 08., 2013.

- Good to do:
  - Do not underestimate the enemy.
  - Continuous analysis.
  - Be unpredictable.
  - Change weapon system, organization structure and TTPs regularly.
  - Keep OPSEC priority.

PRINCIPLE 4:
NEVER LOSE SIGHT OF YOUR OBJECTIVE

- The objective is the central piece of a national strategy.[34] Every leader has to see the direct connection between his organization's objective, and the objectives of at least two echelons higher.[35] Logical relationships must be found because their absence can cause momentous disadvantages. History demonstrates that it is imperative for nations, when they are moving to war, to have a clearly defined objective.
- The objective is in the center of almost every planning model.[36] The objective lives in dialectical balance with ways and means, with methods and resources, with process and materials. Moreover, the objective has to be the logical implementation of the value-based interest and has to support the commander's/leader's intent. Furthermore, the objective is responsible for determining the desired end-state which is the practical manifestation of the main goal.
- The objective must be clear, simple, and easily understandable to subunits, and to collaborative organizations, in order to allow them to make it part of their own plan. The various representatives of national power that are working in the theater to accomplish their mission, and the participants of joint military operations can have only one common objective. This is the essence of the comprehensive approach.
- The comprehensive approach appears to be a global concept that is often associated with civil-military cooperation; however, it goes beyond

---

34   For additional background on the Strategy Formulation Model see *Course Directive – National Security Policy and Strategy.* U.S. Army War College, Carlisle Barracks, PA: 2013, pages 4–7.
35   For additional background see: *Joint Operation Planning.* Chapter IV.
36   The objective can be found in various strategic formulation models under various names, such as goal, aim, or mission. For additional background see: McNAMARA, Carter. *Basic Overview of Various Strategic Planning Models,* http://managementhelp.org/strategicplanning/models.htm, Accessed: December 08., 2013.

the existing NATO doctrine on enhanced civil-military cooperation (CIMIC). Furthermore, it is often mentioned in conjunction with counterinsurgency, Provincial Reconstruction Teams (PRT-Afghanistan), peace operations, stability operations and crisis management.[37]

- Due to the diversity of the possible participants at every level of armed conflict, the objective needs to be as permanent as possible, because the central role of the objective strongly affects planning and execution outcomes. Sometimes the diversity of participants (or, rather, the bias they bring with them), or such personal interests as professional assignment, financial benefit, cultural and religious stereotyping can mislead the execution. Therefore, the importance of the objective is not just a written phrase in various documents, but an essential component that everybody must keep in mind throughout engagement.

Summary of the forth principle:
- Logical connection among objectives at different levels.
- Logical consequence of interest, intent and desired end-state.
- Objective requirements:
  - Clear, simple, understandable, mutual, and permanent.
  - Elimination the human factor such as emotion, hate, revenge, stereotype, and bias.

PRINCIPLE 5:
BUILD AND USE A CLEAR CHAIN OF COMMAND

- Recent and possible future armed conflicts will occur in an extremely complex environment. Multiple participants from military services, governmental and non-governmental organizations, national and international participants are working for the same objective at every level in the same theater. General Dempsey emphasized the importance of the chain of command when he recently stated, that *"in response to these challenges and others, we will lead, and we will enable others to lead. Moreover, we will do this – always – by coordinating military power*

---

37   *NATO Comprehensive Approach*. NATO Multimedia Library, NATO LibGuides, http://natolibguides.info/comprehensiveapproach, Accessed: December 08., 2013

with the diplomacy and development efforts of our government and those of our allies and partners.''[38]

- Unfortunately, multiple chains of command exist in most nations, especially when the entire DIME[39] is employed. It is of great importance that every participant must know the official relationship between the organization and its superior entity, because there is always one common higher command. It must be clear which organization has the higher authority to employ the national or international instruments of power.
- The areas of responsibilities are shared among stake holders due to different professions, experiences, and capabilities therefore the whole chain of command should be as simple as possible without overlapping responsibilities. If this principle is ignored or cannot be realized, that will strongly affect the other principles as well.[40] It can cause wasteful and ineffective use of resources, and can neutralize the efforts and the results achieved earlier by other units and organization.[41]
- The characteristics of modern warfare demand the coordination of multiple missions among diverse participants, therefore, communication among them becomes essential. This was highlighted by Gerald R. Ford, who said: *"Nothing in life is more important than the ability to communicate effectively.''[42]* Active coordination is one of the most significant parts of how decentralized leadership style is put into practical execution. However, centralization and decentralization have to take place in parallel, and not only internally but externally as well, under the leadership of the authority responsible for the echelon and for the area. To find this balance is one of the most difficult challenges of the leader, because his responsibility and authority require access to, and use of, resources,

---

38   DEMPSEY, Martin. "Chairman's Strategic Direction to the Joint Force." February 6, 2012, quoted in: *Course Directive – National Security Policy and Strategy.* U.S. Army War College, Carlisle Barracks, PA: 2013; page 115.

39   DIME is the acronym for the instruments of national power: Diplomacy, Information, Military and Economy.

40   The Author's experience in Afghanistan can serve as an example. Two NGOs from different countries, using the development budget of a third state wanted to initiate similar projects in the same area without former coordination with the Battle Space owner and Afghan Provincial level officials.

41   Figure 1 introduced the diversity of military operations including missions which demand execution without weapon as well.

42   BALDONI, John. *Great Communication Secrets of Great Leaders.* New York: McGraw Hill, 2003; Page xiii

materiel and information, and can influence the first, second and third principles.

Summary of the fifth principle:
- Intergovernmental and international circumstances.
- Simplicity.
- Importance of Liaison officers.
- Balance between centralization and decentralization.

CONCLUSION

The characteristics of war have changed a lot since Clausewitz wrote his book *On War.* The environment of war has become extremely complex, therefore not only the definition but the principles of war must change as well. The most often cited definition of war by Clausewitz is: *"war is only a continuation of state policy by other means."*[43] Even Clausewitz believed that this question was difficult, therefore, he tried to explain his thoughts in an entire book which was not finished due to the complexity of this question.[44]

In a war, participants must apply and use every single instrument of national power, such as diplomatic, economic, military, and information to achieve the desired end state. But this end state comes mainly from interest, based on values. The policy is only the platform to introduce the interests.[45] Unfortunately, these interests may not be equal with national interest because even non-state actors and non-governmental organizations are able to force the official administration to initiate war or armed conflict to achieve their interest. The formula has become more intricate, therefore a reconsideration of the principles of the Clausewitzian age is needed. This essay gave an overview of the importance of shortening our list of principles of war to a relevant, viable number that can be used generally in armed conflict.

In addition, five guidelines to how to think about armed conflict were introduced to help simplify the planning and execution of war-related tasks. This is an acceptable number because of capability of the human mind and

---

43   Clausewitz. *On War.*
44   For additional background see: PERJÉS, Géza. *Clausewitz.* page 10.
45   "In American thinking foreign policy and strategy were compartmentalized into successive phases of national policy." KISSINGER, Henry. *Diplomacy.* New York: Simon and Schuster, 1994; page 402.

the challenge of time pressure. Military operations demand quick reactions therefore principles must keep in mind always to have chance to be successful. These five guidelines can serve as categories including the values of former principles, which are still applicable one by one but not mutually. These five should always be used jointly to reach the desired end-state successfully at every level, in every domain, and by every participant.

> **Romulusz Ruszin** is a Brigadier General of the Hungarian Defence Forces. He was commissioned in 1995 as an artillery officer. He has served in a series of command and staff positions, and served two tours in expeditionary operations (Iraq and Afghanistan). He has also attended several anti-terrorist courses in Hungary and the United States, earned his PhD at the Zrínyi Miklós National Defence University in Budapest in 2010.and graduated from the US Army War College in 2014. In addition to Hungarian he speaks German and English. Currently he commands the 5th Infantry Brigade of the Hungarian Defence Forces.

BIBLIOGRAPHY

Allied Joint Doctrine for The Conduct of Operations, AJP–3(B). NATO Standardization Agency, March 2011.

Allied Joint Doctrine, AJP–01(D), North Atlantic Treaty Organization Standardization Agency, December 2010.

Army Field Manual, FM–3 Military Operations. Washington DC: Headquarters Department Of The Army, 27. February 2008.

BACON, Francis. *The New Organon, Book II.* in The Works of Francis Bacon vol. iv. Cambridge: Cambridge University Press, 2011.

BALDONI, John. *Great Communication Secrets of Great Leaders* New York: McGraw Hill, 2003.

BROWN, Gary D. and TULLOS, Owen W. *On the Spectrum of Cyberspace Operations*, Small Wars Journal, 11. December 2012 – http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations, accessed: December 08., 2013.

Campaign Manual C100–5 – Operations, 3rd Edition, Brasília, Federal District 1997.

Canada's Army, B-gl-300-000 Fp-000 (Cfp 300) Canada's Army, Caf, 2001
– http://www.scribd.com/doc/98779561/B-gl-300-000-Fp-000-Cfp-
300-Canada-s-Army-Caf-2001, accessed 22/10/2013

CLAUSEWITZ, Carl von. *On War.* Princeton: Princeton University Press,
1976.

Course Directive – National Security Policy and Strategy. U.S. Army War
College, Carlisle Barracks, PA: 2013.

DEÁK, János. "Napjaink és a jövő háborúja" (Current and future war),
Hadtudomány, 2005/1. 29–49.

DEMPSEY, Martin. "*Chairman's Strategic Direction to the Joint Force*"
February 6., 2012, quoted in: *Course Directive – National Security
Policy and Strategy.* U.S. Army War College, Carlisle Barracks, PA:
2013.

Doctrine for the Armed Forces of the United States, Joint Publication 1, 25
March 2013.

ETTRICH, Brian B. *The Principles of War: Are they still applicable?* Naval
Postgraduate School, Monterey, California, Thesis, June 2005 calhoun
– nps.edu/bitstream/handle/10945/10011/05Jun_Ettrich.pdf?sequence=1
accessed 07/10/2013

FM 90-26 Airborne Operations. Headquarters, Department of the Army,
December 1990

FUNARO, Kaitlin. *WikiLeaks scandal's Bradley Manning: 'I'm going to die'
in military prison* – http://www.globalpost.com/dispatch/news/regions/
americas/united-states/121129/wikileaks-bradley-manning-im-going-
die-military-, Accessed: December 08., 2013.

GERRAS, Stephen J. "*Thinking Critically about Critical Thinking: A
Fundamental Guide for Strategic Leaders*" in Planner's Handbook for
Operations Design, Version 1.0. Suffolk, VA: Joint Staff, J–7, October
7., 2011.

HALPERN, Diane F. *"Creative Thinking," in Thought and Knowledge:
An Introduction to Critical Thinking, 4th ed.* Mahwah, NJ: Lawrence
Erlbaum Associates, 2002

http://armypubs.army.mil/doctrine/Active_FM.html, Accessed: October 14.,
2013.

http://nsa.nato.int/nsa/nsdd/listpromulg.html, accessed: October 14., 2013.

http://www.napoleon-series.org/research/napoleon/c_quotes.html, accessed:
December 08., 2013.

Joint and National Intelligence Support to Military Operations, Joint Publication 2–01 Washington, DC: US Joint Chiefs of Staff, 05 January 2012; page II–1

Joint Doctrine Publication 0–01: UK Defence Doctrine, Fourth edition, London: Ministry of Defence, 2011.

Joint Operation Planning, Washington DC: Joint Publication 5–0, August 11., 2011.

JOMINI, Antoine-Henri. *The Art of War.* Novato, CA: Presidio Press, 1992.

KISSINGER, Henry. *Diplomacy.* New York: Simon and Schuster, 1994.

KNAUSZ Imre, *A tanítás mestersége (The profession of teaching)* – http://mek.niif.hu/01800/01817/01817.htm, accessed October 07., 2013.

KÓSA, Sándor and RUSZIN, Romulusz. *A harcászati feladatok osztályozása és tartalmuk meghatározása*, *(Types and definitions of tactical tasks)* Budapest, Hadtudomány 2005/3 pages 42–48.

Land Doctrine Publication, Military doctrine for land operations, Netherlands Operation Training Centre, 2009; 6293.

MALLICK, P.K. *Principles of War: Time for Relook*, The Centre for Land Warfare Studies, New Delhi, 2009.

Manual of NATO safety principles for the storage of military ammunition and explosives AASTP–1. North Atlantic Treaty Organization Standardization Agency, May 2010.

McNAMARA, Carter. *Basic Overview of Various Strategic Planning Models,* http://managementhelp.org/strategicplanning/models.htm, Accessed: December 08., 2013.

Military Operations FM–3. Washington DC: Headquarters Department of The Army, 27. February 2008.

NATO Comprehensive Approach. NATO Multimedia Library, NATO LibGuides – http://natolibguides.info/comprehensiveapproach, Accessed: December 08., 2013.

NATO Glossary of terms and definitions (English and French) AAP–06, North Atlantic Treaty Organization Standardization Agency, 2013

NORTH, Gary L. and RIORDAN, John. *The Role of Space in Military Operations: Integrating and Synchronizing Space in Today's Fight.* High Frontier 4, no. 2. February 2008 – http://www.afspc.af.mil/shared/media/document/AFD-080226-050.pdf accessed December 08., 2013.

PANETTA, Leon E. *"Building Partnership in the 21st Century,"* Dean Acheson Lecture, US Institute of Peace, 28. Jun 2012.

Peace Support Operations AJP–3.4.1, North Atlantic Treaty Organization Standardization Agency, July 2001.

PERJÉS Géza. *Clausewitz*, Budapest, Magvető, 1983.

POPE, Alexander. *An Essay on Criticism*, 1709, http://www.phrases.org.uk/meanings/a-little-knowledge-is-a-dangerous-thing.html, Accessed: December 10., 2013.

"*Principles of war in the Soviet Union and Russia*" – http://dictionary.sensagent.com/principles%20of%20war/en-en/ – 30/06/2013.

Ranger Handbook. United States Army, Ranger Training Brigade United States Army Infantry School, Fort Benning, Georgia, April 2000.

RUSZIN Romulusz. *A Magyar Honvédség Tábori Tüzérségének alkalmazási lehetőségei béketámogató műveletek során* (Opportunities for the employment of the field artillery of the Hungarian Defence Force in Peace Support Operations). Zrínyi Miklós National Defense University, Hungary 2009 – http://portal.zmne.hu/download/konyvtar/digitgy/phd/2010/ruszin_romulusz.pdf, accessed October 07., 2013.

SCOWCROFT, Brent. Foreword to: GEORGE, Roger Z. and RISHIKOF, Harvey (eds.) *The National Security Enterprise: Navigating the Labyrinth.* Washington DC: Georgetown University Press, 2011.

Strategic Concept (SC 99/ MC 327/2 (Final), NATO Military Policy for Non-Article 5 CRO, 29 Aug 01.

SUN TZU. *The Art of War.* New York: Oxford University Press, 1963.

The Army (Revised Edition), Army Manual M 1 TD, The Malaysian Army/ Armed Forces, 2010.

The Charter of the United Nations. New York: UN Publications http://www.un.org/en/documents/charter/ accessed May 29., 2013.

"The early years: UN Peacekeeping was born at a time when Cold War rivalries frequently paralyzed the Security Council United Nations official home page, peacekeeping operations." United Nations official home page – http://www.un.org/en/peacekeeping/operations/early.shtml, accessed: December 08., 2013.

Webster's Third New International Dictionary of the English Language Unabridged, G&C Merrian Company, Springfield, Massachusetts, USA, 1961.

GERGELY TÓTH
The Challenge for Ius a(n)d Bellum

ABSTRACT: The legitimacy of armed conflicts is determined by *ius ad bellum,* a body of international law that primarily contemplates the use of (armed) force, and the circumstances in which such use would be legitimate. The Clausewitzian approach to warfare, as well as the experiences of two world wars have shaped the current rules. Wars of the early 2st century made many scholars and practitioners realize that the nature of conflict is changing, thus the law may have to change. This paper examines two areas that will probably be crucial understanding warfare from a legal point of view. One is the question of self-defense and "pinprick" provocations: in cases when individual provocative actions, being examined separately, may not amount to aggression, however, they, taken as a line of events, may justify invoking the right of self-defense is an area of international law that needs more exploration. The other is the internationalization of internal armed conflicts: determination of the character of an armed conflicts is of outmost importance, since the applicable bodies of law (both *ius ad bellum* and *ius in bello*) are largely determined by the classification.

INTRODUCTION

Grey Zone conflicts pose a problem not only for military theorists, but also for lawyers. When preparing for the conference, I was first looking at the question of *Ius ad Bellum*, that is, the body of law that enables or prohibits a party to engage in armed conflict in a lawful way. After finishing the first draft of my presentation, the spell checker corrected "ad" to "and," and it was sent to the organizers that way. Although later the mistake was spotted, it seemed appropriate to give an ambiguous title, as grey zone conflicts are themselves ambiguous.

The novelty of such conflicts is that they actively exploit legal ambiguities as a force multiplier, and by doing this they play constantly on the fringes of the existing legal regime. Thus, while *ius ad bellum* and *ius in bello* are traditionally considered as separate and not overlapping fields of the domain of the law of armed conflicts, in grey zone and hybrid conflicts the two frequently cannot be kept apart. For example, in the case of a military conflict with the pronounced aim of regime change (maybe even supported by legal arguments), can the rules of occupation apply, which generally seek to maintain the social fabric of the occupied territories intact?

Also, by balancing on the border between non-armed conflict situations and an armed conflict (especially in the case of non-international armed conflicts, where the line is already unclear) grey zone conflicts question some of the fundamental principles of the law of armed conflicts, especially regarding distinction between legal classification of situations, as well as distinction between persons (combatant vs. civilian/protected) and objects (military objectives vs. civilian/protected objects) in the theatre of operations.

Another problem, linked to the question of *ius ad bellum* is what amounts to "Crossing the Rubicon:" when can the legal instruments regulating armed conflict be put to work? The issue is complicated, because even while there are fairly standard, elaborated and tested criteria for what amounts to armed conflict, there is always a political element besides the legal one, and it can distort the analysis both ways. A skilled party to a conflict can very well use this ambiguity to always stay behind the red line, not committing to full conflict while still reaching (most) of its goals.

Finally, grey zone and hybrid conflicts often arise in situations when an internal armed conflict is becoming internationalized. There are several legal theories how it can happen, however, the result is never clear, therefore it leaves the parties to interpret it in their own way, creating a situation where the legal evaluation of certain actions is not straightforward. This can greatly contribute to propaganda efforts, which form an important part in today's wars.

Ius ad bellum Questions

Examining the current situation of *ius ad bellum,* it is well known, that – unlike for most of mankind's history – the legal ground to initiate armed hostilities is very narrow today. There are only two internationally recognized possibilities: either self-defence, under Art. 51. of the UN Charter (or, most would say,

also under customary law), or with UN Security Council authorization under Chapter VII of the same Charter. Some scholars may add the rather dubious case of the "Responsibility to Protect (R2P)"[1] to which others would say "humanitarian intervention" under a new name, and probably most would agree that self-defence includes preemption, although its exact extent would be debated, trying to separate it from preventive war.

My goal is not to elaborate the legal nature of *ius ad bellum*, but to point out some of the consequences of this very narrow possibility to "legally wage war." Once a party cannot show the legitimacy of its operations, it may easily be labeled aggressor. The consequences are not only rhetorical: effectively, legal cover can be lost, opening up the way to all sorts of unpleasant consequences.

Against aggression, not only self-defence, but collective self-defence can be used as well, therefore military alliances will start to play a role. Even if some of the allies are hesitant to support the party under attack, if the case of aggression is clear-cut, they have little legal room to maneuver honoring their obligations.

This is well illustrated in the much-talked-about book of General Sir Richard Shireff, former DSACEUR: *War with Russia,* where the Latvian ambassador to NATO says at one point:

> *"The very rules of war have changed and what we are witnessing in Latvia is the role of non-military means of achieving political and strategic goals; war, as it were, by other means. The advantages we in Latvia enjoy as a result of NATO's unconditional guarantee of collective defence are being nullified by the sophisticated application of hybrid or asymmetric techniques..."[2]*

Another consequence may be sanctions, either by the UN, or by a group of willing states. In this case, major powers often also sanction those not willing to apply the sanctions themselves, but for doing so, usually there is a need for solid legal justification.

International criminal law also deals with the crime of aggression, therefore leading political and military figures of the aggressor state can also be liable to individual criminal responsibility.[3]

---

1   63/308 The responsibility to protect. UN General Assembly, 7 October 2009, A/RES/63/308 – http://www.refworld.org/docid/4ad6d1fd2.html [accessed 23. July 2017]
2   SHIRREFF, Richard. *War with Russia.* London: Coronet, 2016.
3   "Definition of the crime of aggression." Global Institute for the Prevention of Aggression – https://crimeofaggression.info/role-of-the-icc/definition-of-the-crime-of-aggression/ [accessed 23 July 2017]

Finally, while in the legal sense there is no connection between *ius ad bellum* legality of an armed conflict and the application of *ius in bello* during the conflict, in the domain of information warfare the aggressor will always be scrutinized more for *ius in bello* violations, therefore its freedom of action will be more limited in waging the conflict.

CROSSING THE RUBICON

So the main question in grey zone warfare is, when and how the Rubicon of aggression will (not) be crossed, in order to capitalize on the disruption caused by the actions of the attacked, but still avoiding the legal niche where self-defence and other powerful legal mechanisms can be invoked.

The current international legal system is built on the assumption that peaceful relations among nations is the normal state of affairs, and (armed) conflict is something of an aberration. Another basic tenet is that war and peace are objective phenomena, therefore it is always possible to distinguish between them.[4] Grey zone conflicts challenge both these – largely unspoken – assumptions. In these conflicts, there is no objective boundary between peacetime and wartime, instead, the whole relationship is viewed by at least one party as a continuous war, by different means. Complicating this issue is that although there is a widely accepted legal threshold for aggression in UN General Assembly Resolution 3314. (1974), the political threshold for labeling someone aggressor is much less clear, therefore leaving room for ambiguity.[5]

Grey zone conflicts often form a part (or a stage) of hybrid warfare operations. In these cases the "aggressor" operates just below the level of actual armed conflict, sometimes using only the very credible threat of armed attack. The legal ambiguity (creating a *status mixtus*) is therefore used as a force multiplier or divider, absorbing significant resources of the enemy while he tries to counter it.

Utilizing legal ambiguities and loopholes also means that actions fail to meet normative expectations, and while surprising the enemy has always been a central element of warfare, breaking accepted rules of warfare has not

4   GROSS, Leo (1948). "The Peace of Westphalia, 1648–1948." American Journal of International Law 42 (1): 20–41 [p. 25]

5   3314. Definition of Aggression. UN General Assembly, 14 December 1974, A/RES/3314 – http://www.refworld.org/docid/3b00f1c57c.html [accessed 23. July 2017]

been an accepted method of gaining advantage. This applies not only to *ius ad bellum*, but also to *ius in bello* situations.

The outcome of this is the creation of an asymmetric legal environment, where exploiting legal thresholds, generating legal ambiguity and even violating legal obligations. However, all these consequences have limited reach, as they mostly affect those directly involved in the conflict. The broader scope is more important, as all these actions are used by propaganda to create narratives and counter-narratives of events. Such actions can have strategic consequences.

LAWFARE

This leads to a phenomenon called lawfare, where legal factors form an important part of the military operations. Law is important not so much in the sense that the parties try to play according to the legal rules, rather, that they try to create the perception that they do so – and their adversary does not. Law therefore becomes a domain of the conflict, mostly connected to information warfare.

As most Western societies are very vulnerable to such propaganda efforts – being "post-heroic" societies,[6] where the population sees warfare as something innately suspicious, and prone to illegal acts – lawfare can become a very important part of the effort, a real force multiplier, even capable of bringing a stronger opponent to its knees, by simply breaking the will of its society to continue investing into the fight.

Looking at the problem on the doctrinal level, it is clear that once a party introduces lawfare into its arsenal, there is a very strong incentive for the other side to follow suit, hoping to counterbalance the situation or even gain an advantage itself. This is evident in NATO's interest in hybrid warfare after seeing Russia taking advantage of these techniques in its "near abroad." The problem with this approach is that in the long term it undermines international legal rules regulating warfare in general, and since the current rules are mostly beneficial to Western-style developed armed forces, in the end it creates a legal environment less conductive than today's.[7]

---

6   LUTTWAK, Edward N. "Toward Post-Heroic Warfare," Foreign Affairs. May/June 1995.
7   SARI, Aurel. "Hybrid Warfare, Law and the Fulda Gap" IN: Complex Battle Spaces. Michael Schmitt, Christopher Ford, Shane Reeves & Winston Williams (eds.). Oxford: Oxford University Press, 2017.

CLASSIFICATION OF CONFLICTS

Finally, there is an area within law that merits closer attention: The *ius in bello* question of classification of armed conflicts. The importance of this issue is that it determines which set of law is actually used in the conflict. Most treaty rules are applicable in international armed conflicts only, while customary rules of international law will generally apply to all situations that are armed conflict.

However, whether there is an armed conflict at all will sometimes depend on classification. For international armed conflict, the threshold for violence is very low – between the right actors (basically, between states) the smallest attack can be considered as an armed conflict. In some cases – occupation with no resistance but no consent either – even non-violent actions can trigger the application of the law of war. On the other hand, in a non-international armed conflict, there is a certain level (intensity and length) of violence that is required for it to be considered an armed conflict instead of domestic criminal activities.[8] To even further complicate the issue, state and government recognition can blur this picture in actual cases, somehow invoking the old notion of recognition of belligerent status which can be based on political considerations instead of strictly factual and legal arguments.

There are many theories that try to internationalize internal armed conflicts – many of them found their way into decisions of international tribunals. The purpose of these applications – and some would say, extensions – of the rules regulating international armed conflict was to provide protection to victims of armed conflicts that were not clearly international, however, they had elements that made them different from simple non-international conflicts.

The International Criminal Tribunal for the Former Yugoslavia (ICTY) put ethnicity (as nationality was not available, all warring parties belonging to the same state) as the factor that internationalized an otherwise internal conflict. By doing this, they were able to apply the Fourth Geneva Convention of 1949, although some would say that in fact it was a *contra legem* interpretation of the law.[9]

---

8   *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*, 8. June 1977, International Committee of the Red Cross (ICRC), 1125 UNTS 609 – http://www.refworld.org/docid/3ae6b37f40.html [accessed 23. July 2017]

9   Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999 – http://www.refworld.org/cases,ICTY,40277f504.html [accessed 23. July 2017]

Another possibility is to invoke Art. 1. para 4. of the First Additional Protocol to the Geneva Conventions. However, as colonial liberation wars are practically over (in fact, most of them were already over when the Additional Protocol was adopted in 1977), there is little possibility of utilizing this provision.[10]

Some theories, especially in jurisprudence, propose to set up a middle category for internationalized non-international armed conflicts, but these are only *de lege ferenda* proposals, therefore have little practical value at the moment.

For outside third parties, becoming involved on the non-governmental side of a non-international armed conflict, both the International Court of Justice (ICJ) and the ICTY developed tests, based on the concept of state responsibility. The ICJ required effective control[11] of the anti-government side by the outside party, while the ICTY was less stringent when required only overall control.[12] These two approaches both aim to establish a link that can serve as an important indicator in grey zone conflicts However, their usefulness is dubious regarding enabling application of *ius in bello* rules.

Nevertheless, putting into perspective all the above theories, we can safely assume that faithful application of Common Art. 3. of the Geneva Conventions of 1949 – the "mini-convention" Article, that regulates non-international armed conflicts – would already be a huge step ahead in non-international armed conflicts.

Conclusion

To sum up the relations between *ius* and *bellum,* between law and war in grey zone conflicts, we can safely say, that using – and abusing – the law is an integral part of this type of conflicts. It is the ambiguity, both in legal and real-life terms that characterizes this sort of engagement between actors (states and non-state actors alike), and ambiguity is used as a strategic enabler or disabler.

---

10   *Protocol Additional to the Geneva Conventions.*
11   Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986– http://www.refworld.org/cases,ICJ,4023a44d2.html [accessed 23. July 2017]
12   Prosecutor v. Dusko Tadic aka „Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction), IT-94-1, International Criminal Tribunal for the former Yugoslavia (ICTY), 2 October 1995 – http://www.refworld.org/cases,ICTY,47fdfb520.html [accessed 23. July 2017]

Countering this type of warfare is not easy, as it does not conform to some basic tenets of the Westphalian legal order, namely, that peace is the norm in international relations, and that war and peace are objective phenomenon that can be separated from each other. There is a great temptation to for the party being subject to such methods to emulate them. However, western nations should be careful not to go down this slippery slope, because in the end, they have more to lose than to gain. Constant application of such bending of the rules would finally undermine the existing international legal order which is designed to mostly benefit Western developed countries and their armed forces.

Another takeaway may be, that as law becomes a domain of warfare (maybe as a subset of information warfare) it is imperative to dominate this domain, like other domains are to be dominated. This requires good military lawyers and legal services, more prepared than ever.

BIBLIOGRAPHY

3314. Definition of Aggression. UN General Assembly, 14 December 1974, A/RES/3314 – http://www.refworld.org/docid/3b00f1c57c.html [accessed 23. July 2017]

63/308 The responsibility to protect. UN General Assembly, 7. October 2009; A/RES/63/308 – http://www.refworld.org/docid/4ad6d1fd2.html [accessed 23. July 2017]

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27. June 1986 – http://www.refworld.org/cases,ICJ,4023a44d2.html [accessed 23. July 2017]

"*Definition of the crime of aggression*" Global Institute for the Prevention of Aggression – https://crimeofaggression.info/role-of-the-icc/definition-of-the-crime-of-aggression/ [accessed 23. July 2017]

GROSS, Leo (1948). "*The Peace of Westphalia, 1648–1948*" American Journal of International Law 42 (1): 20–41 [p. 25]

LUTTWAK, Edward N. "*Toward Post-Heroic Warfare*" Foreign Affairs. May/June 1995.

Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15. July 1999 – http://www.refworld.org/cases,ICTY,40277f504.html [accessed 23 July 2017]

Prosecutor v. Dusko Tadic aka „Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction), IT-94-1, International Criminal Tribunal for the former Yugoslavia (ICTY), 2. October 1995 – http://www.refworld.org/cases,ICTY,47fdfb520.html [accessed 23. July 2017]

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8. June 1977; International Committee of the Red Cross (ICRC), 1125 UNTS 609 – http://www.refworld.org/docid/3ae6b37f40.html [accessed 23. July 2017]

SARI, Aurel. "*Hybrid Warfare, Law and the Fulda Gap*" IN: Complex Battle Spaces. Michael Schmitt, Christopher Ford, Shane Reeves & Winston Williams (eds.). Oxford: Oxford University Press, 2017.

SHIRREFF, Richard. *War With Russia*. London: Coronet, 2016.

For nearly seven decades the political cohesion and military power of the NATO alliance has ensured the prosperity and security of the Euro-Atlantic region. However, today resurgent and emerging powers, as well as non-state entities are aggressively opposing the alliance in ways that are often far from peaceful, but fall short of any recognized threshold of conventional war. These confrontations pose a particular difficulty both for NATO as a whole, and for some of its member states, since their political and military structures are optimized for prevailing in conventional conflicts. The biggest challenge is that the Alliance needs to operate and adapt at the same time.

The conference organized by Scientific Research Centre of the Hungarian Defence Forces General Staff addressed this phenomenon, the spectrum of gray zone challenges, as well as the possible NATO and nation-state responses to them. The presentations and panel discussions gave partial answers to the questions concerning the emerging security environment, as well as the necessary social and adninistrative responses, and the possible military responses to Gray Zone challenges. This volume contains the papers that were presented during the conference, as well as the conclusions and policy recommendations that the participants developed in the course of panel discussions and plenary debate.