Conference Conclusions

Conflicts in the Gray Zone

A Challenge to Adapt

May 9-10 2017, Budapest, Hungary

Hungarian Defence Forces General Staff, Scientific Research Centre

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. The organizers plan to publish the proceedings of the conference, once the speakers submit their papers. The expected date of publication is early September 2017. While the proceedings are being prepared, this publication is offered as the conclusions and recommendations for policy makers by the conference participants.

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.”

Abstracts of Presentations

Peter Balogh: Gray Zone Activities – with a Focus on the Social Domain

(Hungary, University of Szeged)

The presentation outlines the diverse theoretical background of the Gray Zone/hybrid competition, and links it to further concepts from social sciences, which reflect the importance of the societal aspect and assist in grasping the processes behind Gray Zone activities. Addressing the macro level, the presentation outlines results from an empirical study of international terrorism with an emphasis on the countermeasures and the global war on terror. The observation that some of the countries committed to fight global terrorism are working against their partners in other activities illustrates the ambiguity of Gray Zone. Addressing the subnational level, it also sheds some light on how hybrid competition, the civil sector and bottom-up social movements, the political domain and mass media are interconnected. A certain 'whitening' of the Gray Zone can be observed in the Hungarian (and European) media: not only do hybrid aggressors rely on politics but political interest groups also attempt to take advantage of the activity of Gray Zone adversaries. The conclusion is that Gray Zone activities are becoming a part of the public agenda.

Lazar Berman and Yaniv Friedman: The Suppressed Sword: Legitimacy Challenges in Gray Zone Conflict

(Israel, Dado Center for Interdisciplinary Military Studies)

Israel, the US and other Western powers struggle to use their considerable military might against weaker actors because they often lack the international and internal legitimacy to do so. Gray zone conflict holds 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. The paper examines the unique challenge of legitimacy – and by extension deterrence – in gray zone conflicts, drawing insight from contemporary and historical Israeli experience. It also seeks to provide an approach for Western responses to the legitimacy challenge.

Luís Manuel Brás Bernardino: Africa's Grey Zone: the Sahel

(Portugal, Military Academy)

Africa's Sahel region is one of the most complex and interconnected challenging region in the African continent. A huge region were 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 zone in Africa and in the world. In this multi-complex 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 witch, 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.

Matthew Domingos and Kerin Winiarz: Warfare by Proxy

(USA, Joint Staff J7)

Through analysis of historical case studies spanning the last 50 years the paper isolates the key principles that lead to a nation's successful or unsuccessful use of proxy warfare to achieve national objectives. It also identifies the characteristics of, and possible tensions in, the patron-proxy relationship. It presents a qualitative analytical to assess and understand the contemporary use of proxy warfare as part of the gray zone. Most importantly, it provides a framework and foundation to future research on ways to develop resilience in the face of proxy warfare use in the gray zone.

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

(Hungary, Corvinus University of Budapest)

The paper provides an overview of how armed conflicts of the 21st century (especially the experience gained in Ukraine and in Syria) are perceived in contemporary military thinking in the Russian Federation. A review of Russian foreign and security policy publications, journals of military science, policy documents (the military doctrine, etc.), the declarations of leading officials, and publicly available information on Russian military exercises held since 2013 are assessed to map out the types of conflict the Russian military has been preparing for.

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

(USA, George Mason University)

A key issue in developing military Courses of Action that fit within a national response is understanding the adversary's intent. However, that intent is often ambiguous and often the ambiguity is deliberate. One way to reduce the ambiguity is to consider an Indications and Warning (I&W) framework of impending crises for specific Gray Zone actors and their targets. Once the indications and warning activities have been identified, they can be used by a nation and its partners to develop Courses of Action to proactively counter in order to prevent or mitigate a Gray Zone competitor trigger. Tools and techniques exist for embedding the military option in the broader national and partner Course of Action options. It is possible to represent simultaneously the set of possible adversary intents and then consider the effect that the various actionable events that are contained within a COA will have.

Spencer B. Meredith III: Governing in the Gray Zone: Reducing Strategic Vulnerabilities by Shaping the Human Domain

(USA, National Defense University, College of International Security Affairs)

The 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, revolving around 1) social values, 2) overlapping and sometimes conflicting identities, and 3) desired goals and the methods required to achieve them. It explores key state approaches to influence this human operational environment. In particular, the paper discusses aspects of statecraft that relate to effective governance, to building societal resistance and resilience, to reducing state vulnerabilities. Case studies show successful strategies in action.

Michael Miklaucic: Paradigm Shift

(USA, National Defense University, Institute for National Strategic Studies)

Contemporary conflict demands that a re-examination of the western understanding of war and of peace. The emergence of highly disruptive non-state actors, often networked with corrupt state actors, threatens the state-centric global system and contributes to an emerging alternative global ecosystem. This paper surveys the emerging alternative ecosystem, describes the variant elements of the new paradigm, as well as demonstrates their increasing convergence, and the threat such convergence poses to national and international security. Since this challenge constitutes a "wicked problem," new concepts of victory and defeat are needed to help policy-makers determine whether or not policies are effective.

Molly Nadolski: A Sociotechnical Modeling Framework for Complex Systems Analysis of Gray Zone Warfare

(USA, Georgia Tech Research Institute)

Despite strides in techniques for assessing problem spaces, using risk management, network science, or development, our collective understanding of increasingly complex domains remains nascent. The limitations of the theoretical frameworks, statistical, and qualitative methods for testing theories of strategic interaction and comparative foreign and security policies are conspicuous in the study of Russian foreign and security policies. The presentation introduces an analytical framework and toolset that decision makers can use to assess complex problem spaces, 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.

Imre Porkoláb: NATO's future vision for fighting in the Gray Zone: a Persistent Federated Approach

(Hungary, Hungarian Defence Force)

The presentation focused on organizational and leadership challenges, which are rapidly changing in the contemporary context. It covered three areas (1) a quick introduction of the main problems associated with contemporary Grey Zone Conflicts (2) A theory of the contextual strategic approaches (3) NATO's vision for organizational transformation in a VUCA environment (a Persistent Federated Approach),. The main theories presented were a framework to better understand the VUCA context, NATO's Persistent Federated Approach, and an Integrated Strategic approach supported by Mission Command 2.0. 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 is necessary to tackle contemporary challenges, and leader development, talent management must be reimagined.

Romulusz Ruszin: Are the Current Principles of War Still Applicable?

(Hungary, Hungarian Defence Force)

The art of war and the principles of armed conflict have been pondered across the millennia. Today's armies are largely influenced by the ideas that emerged from the Napoleonic era. However, the 21st century`s armed conflict environment 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 suggests 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.

Gergely Tóth: Gray Zone Conference: The Challenge to *Ius a(n)d Bellum*

(Hungary, Hungarian Defence Force)

Ius ad bellum is the body of international law that governs the legitimacy of armed conflicts. As the nature of conflict is changing, law will have to change as well. This paper examines two areas that will be crucial for understanding warfare from a legal point of view. One is self-defense and "pinprick" provocations, when individual actions, examined separately, may not amount to aggression, but as a line of events they may justify invoking the right of self-defense. The other is the internationalization of internal armed conflicts. In recent years it is becoming harder and harder to distinguish between these two genres, due to the reason and many internal conflicts have elements that link one or the other party (parties) to external actors.