CONNECTIONS WINTER-SPRING 2019

CONNECTIONS

THE QUARTERLY JOURNAL

PARTNERSHIP FOR PEACE CONSORTIUM OF DEFENSE ACADEMIES AND SECURITY STUDIES INSTITUTES

DETERRENCE IN INTERNATIONAL SECURITY: THEORY AND CURRENT PRACTICE

EDITOR: TODOR TAGAREV

WINTER-SPRING 2019

Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

The PfP Consortium Editorial Board

Sean S. Costigan	Editor-In-Chief
Marcel Szalai	Managing Editor
Aida Alymbaeva	International University of Central Asia, Bishkek
Pal Dunay	George C. Marshall Center, Garmisch-Partenkirchen
Philipp Flury	Geneva Centre for Security Policy, Geneva
Piotr Gawliczek	Cuiavian University in Wloclawek, Poland
Hans-Joachim Giessmann	Berghof Foundation, Berlin
Dinos Kerigan-Kyrou	Joint Command & Staff Course, Military College, Irish Defence Forces
Chris Pallaris	i-intelligence GmbH, Zurich
Tamara Pataraia	Civil Council of Defense and Security, Georgia
Todor Tagarev	Bulgarian Academy of Sciences, Sofia
Eneken Tikk	Cyber Policy Institute, Jyväskylä

The views expressed and articles appearing in all *Connections* publications are solely those of the contributing authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

This edition is supported by the United States government. The Consortium's family of publications is available at no cost at http://www.connections-qj.org. If you would like to order printed copies for your library, or if you have questions regarding the Consortium's publications, please contact the PfPC at PfPCStratCom@marshallcenter.org.

Dr. Raphael Perl	Sean S. Costigan
Executive Director	Editor-In-Chief and Chair, Editorial Board

ISSN 1812-1098, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

Vol. 18, no. 1-2, Winter-Spring 2019

Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

Creative Commons BY-NC-SA 4.0

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

https://doi.org/10.11610/Connections.18.1-2

Contents

Vol. 19, no. 1-2, Winter-Spring 2019

Creative Commons BY-NC-SA 4.0

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Todor Tagarev, *Connections QJ* 18, no. 1-2 (2019): 5-10
https://doi.org/10.11610/Connections.18.1-2.00

Editorial

Theory and Current Practice of Deterrence in International Security

Todor Tagarev

Centre for Security and Defense Management, Institute of ICT, Bulgarian Academy of Sciences, http://www.iict.bas.bg/EN

Abstract: The theory of deterrence emerged with the advent of nuclear weapons to address the challenges of preparing for and preventing a full-scale nuclear war between the United States and the Soviet Union. The contributions to this special issue are set in a post-Cold war context, with a resurgent and aggressive Russia. The set of articles provides an outline of the theory of deterrence, the current practice of its application in deterring and, if necessary, defending by conventional forces NATO and Europe's Eastern flank against aggression, and critical analysis of its pertinence to cyber and hybrid warfare.

Keywords: deterrence, NATO, Eastern flank, forward presence, conventional forces, cyber domain, cybersecurity, cyber operations, legal framework, hybrid influence.

Deterrence has been practiced over the centuries to dissuade an opponent considering a coercive course of action, e.g., an armed attack. The concept became subject of rigorous debates with the advent of the nuclear weapons. By the 1960s, the works by Bernard Brodie,[1] Herman Kahn,[2] Glenn H. Snyder,[3] Thomas

[1] Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Company, 1946); Bernard Brodie, *Strategy in the Missile Age* (Santa Monica, CA: RAND, 1969).

[2] Herman Kahn, *On Thermonuclear War* (Princeton: Princeton University Press, 1960).

[3] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961).

Creative Commons BY-NC-SA 4.0

C. Schelling,[4] and others formed a body of knowledge allowing to elaborate strategies and policies for the nuclear standoff during the Cold war and to avoid a nuclear war.

The application of the theory of deterrence during the Cold war led to an equilibrium between the nuclear arsenals of the two leading nuclear powers—the Soviet Union and the United States of America—guaranteeing that in a full-scale nuclear war, both the attacker and the defender will be annihilated.[5]

With the nuclear détente and the end of the Cold war, the interest in the theory of deterrence subsided. In practice, it was still guaranteed, albeit at lower force levels. For example, while at the end of the Cold war the United States maintained some 7,300 nuclear weapons deployed in Europe to provide security guarantees to NATO Allies, that force has been reduced by 90 percent since then.[6]

The interest in deterrence was renewed in recent years. One reason was the suspension of the Intermediate-Range Nuclear Forces (INF) Treaty at the beginning of 2019[7] and the forthcoming expiration of the New Strategic Arms Reduction Treaty (new START),[8] and the need to find a new balance with an account of the nuclear capacity of other players, China in particular.[9] Another reason is the illegal annexation of the Crimean Peninsula by the Russian Federation and its aggressive cyber and hybrid actions against NATO allies and partners.

This special issue of *Connections: The Quarterly Journal* is focused on the latter and the use of conventional, cyber, and disinformation means to deter aggression.

In the first contribution, Col. Darrell Driver, Director of European Studies at the US Army War College, lays the foundation by reviewing the theoretical foundation of deterrence and its two main underlying concepts – deterrence by pun-

---

[4] Thomas C. Schelling, *The Strategy of Conflict*, with a new preface by the author (Cambridge, MA: Harvard University Press, 1980); Thomas C. Schelling, *Arms and Influence*, with a new preface and afterword (New Haven: Yale University Press, 2008).

[5] James E. Doyle, "Why Eliminate Nuclear Weapons?" *Survival* 55, no. 1 (2013): 7-34, https://doi.org/10.1080/00396338.2013.767402; Tom de Castella, "How Did We Forget about Mutually Assured Destruction?" *BBC News*, February 15, 2012, https://www.bbc.com/news/magazine-17026538.

[6] Jessica Cox, "Nuclear Deterrence Today," *NATO Review*, June 8, 2020, www.nato.int/docu/review/articles/2020/06/08/nuclear-deterrence-today/index.html.

[7] Simon Lunn and Nicholas Williams, "The Demise of the INF Treaty: What Are the Consequences for NATO," *Policy Brief*, European Leadership Network, February 11, 2019, https://www.europeanleadershipnetwork.org/policy-brief/the-demise-of-the-inf-treaty-what-are-the-consequences-for-nato/.

[8] Kingston Reif, "New START at a Glance," *Fact Sheets & Briefs*, Arms Control Association, January 2020, https://www.armscontrol.org/factsheets/NewSTART.

[9] Lunn and Williams, "The Demise of the INF Treaty.

ishment and deterrence by denial.[10] On that basis, Dr. Driver critically evaluates NATO's posture on its Eastern flank and concludes that through the "enhanced forward presence" in the Baltic states and Poland, the "tailored forward presence" in Bulgaria and Romania, the regular exercises in the Black Sea, the creation of the Very High Readiness Joint Task Force (VJTF), and the establishment of NATO Force Integration Units (NFIUs) in the seven Eastern flank states, Allies have already put their "skin in the game" thus ensuring a unified Alliance response in an act of aggression and making NATO retaliation unavoidable. With the increase of defense budgets in line with the Wales pledge, the European Deterrence Initiative of the United States, the so-called "four-30s" decision at the NATO Brussels summit and the development of the "Military Schengen" in Europe Allies are already moving from deterrence by punishment towards deterrence by denial.

Col. Driver also reminds us of the defense and deterrence requirements formulated by Lieutenant General (ret.) Ben Hodges, former US Army Europe Commander, for assuring effective early warning, capable national forces, and adequate infrastructure and prepositioned supplies.[11] Velizar Shalamanov, Pavel Anastasov, and Georgi Tsvetkov develop that point further, starting with the defense pledge from Wales and its implementation at national level on the example of Bulgaria.[12] Then the authors review the experience of defense collaboration in Eastern and South-Eastern Europe, emphasize the advantages of multinational acquisition of the requisite capabilities, and provide a detailed examination of potential multinational formats, initiatives, and funding sources, focusing on the acquisition of information and communication technologies, sensors and command control systems, or C4ISR systems, and multinational education and training. Multinational formations at tactical level and acquisition projects, implemented in a NATO and/or EU format, will contribute interoperable capabilities and solidarity, and thus to the more efficient defense of Europe's Eastern flank.

In the third article in this issue, Rosław Jeżewski sets the ground for discussion on the applicability of the concept of deterrence of coercive actions employing a set of hybrid tools.[13] In the case of Latvia, the author demonstrates how Russia attempts to influence the national course in her interest by combining economic

---

[10] Darrell W. Driver, "Deterrence in Eastern Europe in Theory and Practice," *Connections: The Quarterly Journal* 18, no. 1-2 (2019): 11-24.

[11] Ben Hodges, Janusz Bugajski, and Peter B. Doran, "Securing the Suwałki Corridor: Strategy, Statecraft, Deterrence, and Defense" (Washington, DC: Center for European Policy Analysis, July 2018).

[12] Velizar Shalamanov, Pavel Anastasov, and Georgi Tsvetkov, "Deterrence and Defense at the Eastern Flank of NATO and the EU: Readiness and Interoperability in the Context of Forward Presence, *Connections: The Quarterly Journal* 18, no.1-2 (2019): 25-42.

[13] Rosław Jeżewski, "Cross-domain Coercion as Russia's Endeavor to Weaken the Eastern Flank of NATO: A Latvian Case Study," *Connections: The Quarterly Journal* 18, no. 1 (2019): 43-60.

and financial influence, corruption, exploitation of the minority of citizens of Russian origin, propaganda and disinformation campaigns, the Russian-based organized crime, and large-scale military exercises at the country's borders. The author provides ideas of how to protect against, if not deter, such coercive activities, including examples from Finland's experience. Yet, he concludes by foreseeing that "cross-domain coercion will increase and Russia will test the cohesion of NATO."

Cyberattacks and disinformation campaigns in online media are among the main tools for hybrid influence. The following two articles focus on the applicability of the concept of deterrence to the cyber domain. First, Mika Kerttunen from the Cyber Policy Institute in Tartu, Estonia, critiques the theory of deterrence generally and its applicability to cyberspace.[14] Among the rationale for the latter, the author points to the changed context for cyber deterrence (compared to the use of nuclear weapons), the respectively higher degree of tolerance to cyberattacks, the broader spectrum of approaches to deterrence, and the more nuanced tools, including positive agendas with rewards. In his conclusion, Mr. Kerttunen states that "deterrence is a cumbersome and inappropriate tool to understand the cyber realm."[15]

On the other hand, Manuel Fischer posits that even though the cyber domain requires some special considerations, deterrence as a "classical tool" in international relations can bolster national security interests.[16] Fischer, a graduate of the Master's program of International Security Studies of George C. Marshall European Center for Security Studies, reviews the implications of the concept of deterrence to the cyber domain along six factors—time, available 'forces' (responsible organizations; with consideration of supply chain vulnerabilities), survival, defense tools and capacity, and the challenges of attribution—followed by an examination of the legal framework for involving cyber activities in international relations. Based on the analysis presented in this special issue, Fischer concludes that "[e]ven in the cyber age, deterrence can be a powerful tool of statecraft and contribute to the protection of a state's national security interests!"[17]

While Mika Kerttunen and Manuel Fischer seem to hold opposing views, their findings are not that different. Although to a different degree, both authors see the limitations of *deterrence by punishment/retaliation* in cyberspace and give preference to deterrence by denial, including through relevant network design, better protection, enhancing resilience, public-private partnerships, etc. They also see the value of more positive approaches, the need to strengthen international regimes to provide for "deterrence by normative taboos" and building on

---

[14] Mika Kerttunen, "Beyond Punishment: Deterrence in the Digital Realm," *Connections: The Quarterly Journal* 18, no. 1 (2019): 61-68.

[15] Kerttunen, "Beyond Punishment: Deterrence in the Digital Realm," 67.

[16] Manuel Fischer, "The Concept of Deterrence and its Applicability in the Cyber Domain," *Connections: The Quarterly Journal* 18, no. 1 (2019): 69-92.

[17] Fischer, "The Concept of Deterrence and its Applicability in the Cyber Domain," 70.

the interdependencies in the international system, or the so-called "deterrence by entanglement."[18]

The contribution by Tamara Maliarchuk, Yuriy Danyk, and Chad Briggs examines the use of cyberattacks against the energy infrastructure as one of the tools in the toolbox used by the Russian Federation in its continuing standoff with Ukraine.[19] Current Ukrainian doctrine addresses such cyberattacks (advanced persistent threats, attacks on industrial control systems) along with the use of social networks, attacks on the banking system, and the exploitation of supply chain vulnerabilities. Along the lines of the previous two articles in this issue, the authors identify better protection, resilience, and supply chain security as key for defending against cyberattacks.

Vesna Pavičić wraps up this issue with an examination of Serbia's positioning in the international arena.[20] While the European integration seems the obvious choice, the interests of players like Russia and China, and the instruments they use to promote their interests (in particular those used by Russia – sophisticated propaganda with references to historical ties, orthodox Christianity, the position on Kosovo's independence, dependence on the delivery of gas and oil, defense cooperation, etc.), make Serbia's future path uncertain. The author sees the remedies against the hybrid influence in comprehensive security, political, and economic dialogue with the European Union, stronger civil society, more transparent and free press, and shifts in the political rhetoric.

* * *

This special issue provides an overview of the theory of deterrence and its applicability on NATO and Europe's Eastern flank, vis-à-vis the aggressive policy and actions of the Russian Federation that include use of armed forces against NATO partners, Ukraine and Georgia, and more sophisticated cyberattacks and hybrid influence operations against both NATO members and partners.

The articles included here are focused on the use of conventional forces, cyber means, and ways to enhance the resilience of the armed forces, the economy, and society. Less attention has been paid to the application of the concept of deterrence to a full spectrum hybrid warfare,[21] the role of nuclear weapons in

[18] Fischer, "The Concept of Deterrence and its Applicability in the Cyber Domain," 90.

[19] Tamara Maliarchuk, Yuriy Danyk, and Chad Briggs, "Hybrid Warfare and Cyber Effects in Energy Infrastructure," *Connections: The Quarterly Journal* 18, no. 1 (2019): 93-110.

[20] Vesna Pavičić, "Serbia's Orientation Challenge and Ways to Overcome It," *Connections: The Quarterly Journal* 18, no. 1 (2019): 111-127.

[21] Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs* 92, no.1 (2016): 175-195; Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica, CA: RAND, 2017).

preventing *fait accompli*, reverse or preserve the gains of a hybrid operation,[22] and the interplay of cyber/hybrid attacks and nuclear threats. All these topics merit further consideration in a future special issue of *Connections: The Quarterly Journal*.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Todor Tagarev is a professor in the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences and Head of its Centre for Security and Defense Management. An engineer by education, Prof. Tagarev combines governmental experience with sound theoretical knowledge and background in cybernetics, complexity, and security studies – a capacity effectively implemented in numerous national and international multidisciplinary studies, including ongoing Horizon 2020 projects in the fields of crisis management and cybersecurity. https://orcid.org/0000-0003-4424-0201

[22] Peter Apps, "Commentary: Putin's Nuclear-tipped Hybrid War on the West," Reuters, March 2, 2018, https://uk.reuters.com/article/us-apps-russia-commentary-idUKKCN1GD6H2; Gustav Gressel, "Protecting Europe against Hybrid Threats," *Policy Brief*, European Council on Foreign Relations, June 25, 2019, https://ecfr.eu/publication/protecting_europe_against_hybrid_threats/.

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Darrell Driver, *Connections QJ* 18, no. 1-2 (2019): 11-24
https://doi.org/10.11610/Connections.18.1-2.01

Research Article

Deterrence in Eastern Europe in Theory and Practice

Darrell Driver

United States Army War College, Carlisle Barracks, Pennsylvania, https://www.armywarcollege.edu/

Abstract: This article explores the continuities and changes between Cold War deterrence concepts and approaches and those being employed on NATO's Eastern flank today. It is argued that classic approaches to deterrence, curated in a rich Cold War intellectual tradition, have been clearly on display in NATO's responses to Russian aggression and threats, and it is possible to understand the decisions being made in Brussels and Alliance capitals through a consideration of such classical deterrence concepts as deterrence by denial and deterrence by punishment or direct versus extended deterrence. Concepts like these and others explored here remain useful. Nevertheless, important changes in the scope and nature of the threat must be considered, especially as this pertains to non-military aspects of deterrence and so-called hybrid or 'gray-zone' threats. This will require a merging of traditional concepts of deterrence with the more recent focus on developing a comprehensive approach to contemporary security challenges.

Keywords: deterrence, denial, NATO, Eastern Europe, hybrid threats.

Most people are familiar with the two primary symbols of the transatlantic Alliance: the acronym NATO or l'OTAN and the NATO star. However, there is also an equally old and venerable, if informal, NATO symbol that bears some consideration in any discussion of deterrence and defense: the hedgehog. First mentioned by Dwight Eisenhower in 1951, the first Supreme Allied Commander Europe (SACEUR) encouraged individual Allies to be capable of making themselves into a "hedgehog of defense" in order to buy the time NATO would need to come to their defense. Since the Russian annexation of Crimea in 2014, this long dis-

Creative Commons BY-NC-SA 4.0

carded symbol of deterrence has made a resurgence. However, while this necessary rediscovery of deterrent concepts is underway, there is also much that is different about deterrence and collective defense today that warrants consideration. Borrowing from Isaiah Berlin's famous "fox and the hedgehog" metaphor,[1] changes in the contemporary security environment mean that NATO will require more of the fox's adaptiveness of thought and varied approach to problem-solving as it re-commits itself to a hedgehog-like focus on deterrence.

This article explores both the continuities and changes that warrant consideration in any discussion of deterrence and defense in today's Eastern Europe. I argue that classic approaches to deterrence have been at work in Allies' responses to Moscow's aggression, and it is possible to understand the decisions being made in Brussels and Alliance capitals through a consideration of these classic deterrence concepts. Nevertheless, important changes in the scope and nature of the threat must be considered, especially as this pertains to non-military aspects of deterrence and so-called hybrid or "gray-zone" threats.

Concepts of Deterrence

The concept of deterrence is perhaps as old as human conflict itself, but its intellectual "golden era" was cultivated in the climate of the Cold War from about 1946 to the late 1980s. This period saw the adoption of cornerstone contributions by figures such as Bernard Brodie, Herman Kahn, Thomas Schelling, and Glenn Snyder.[2] Though the driving force behind much of the early work from this period was the advent of nuclear weapons, deterrence as a concept was quickly expanded to the conventional domain as well.[3] Whether nuclear or conventional, the essence of deterrence, according to US joint doctrine, is "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits.[4] Glenn Snyder described deterrence simply as "discouraging the enemy from taking military action by posing for him a prospect of cost and risk outweighing his per-

---

1 Isaiah Berlin, "The Hedgehog and the Fox: An Essay on Tolstoy's View of History," *The Proper Study of Mankind: An Anthology of Essays*, ed. Henry Hardy and Roger Hausheer (New York: Farrar, Straus, and Giroux, 1998). For a more recent use of the metaphor applied to strategy, see John Lewis Gaddis, *On Grand Strategy* (New York: Penguin Press, April 2018).

2 Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Company, 1946); Herman Kahn, *On Thermonuclear War* (Princeton: Princeton University Press, 1960); Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterward* (New Haven: Yale University Press, 2008); Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961).

3 For a focused look at conventional aspects, see John J. Mearsheimer, *Conventional Deterrence* (Ithaca, N.Y.: Cornell University Press, 1983).

4 *DOD Dictionary of Military and Associated Terms*, US Joint Chiefs of Staff, Military and Electronic Library, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

spective gain."[5] Deterrence differs from compellence, the other form of coercion, in that it does not seek to encourage another actor to do something, rather to get that actor to maintain the status quo, to "just keep doing what you are doing."[6] From this basic observation about the purpose of deterrence grew a rich and diverse literature that would be impossible to explore fully in an article of this length. Instead, I would like to focus on few central concepts and approaches worth highlighting for the present problem set.

First, the literature draws a distinction between *Immediate* and *General Deterrence*. "Immediate deterrence, according to Patrick Morgan, "concerns the relationship between opposing states where at least one side is seriously considering an attack while the other is mounting a threat of retaliation in order to prevent it."[7] For this reason, Richard Lebow and Janice Stein label immediate deterrence "a strategy of conflict management" with one side attempting to dissuade the other from aggression.[8] This can be contrasted with general deterrence, which Morgan describes as relating more "to opponents who maintain armed forces to regulate their relationship even though neither is anywhere near mounting an attack."[9] With a few high tension exceptions, like the 1962 Cuban Missile Crisis, Lawrence Freedman argues that this "long haul" deterrence characterized the balance of power relationship and Cold War strategy. According to Freedman, "general deterrence is practiced in order to avoid having to practice immediate deterrence."[10]

The second prominent concept in the literature has to do with the distinction between *deterrence by punishment* and *deterrence by denial*. Deterrence by punishment requires one to convince an adversary that any aggression, initially successful or not, will be met with a response that is unacceptably costly. This approach involves convincing the adversary of both the capability to impose such cost as well as the will to follow through, even in the face of further retaliation. Punishment is different from deterrence by denial, which seeks to demonstrate a credible ability to prevent the adversary from achieving desired objectives in the first place. The US Secretary of State from the early Cold War, Dean Acheson, described the practical difference this way, "we mean that the only deterrent to the imposition of Russian will in Western Europe is the belief that from the out-

---

5 Snyder, *Deterrence and Defense*, 35.

6 Robert J. Art and Kelly M. Greenhill, "Coercion: An Analytic Overview," in *Coercion: The Power to Hurt in International Politics*, ed. Kelly M. Greenhill and Peter Krause (New York: Oxford University Press, 2018), 5.

7 Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage Publications, 1977), 28.

8 Richard Ned Lebow and Janice Gross Stein, "Beyond Deterrence," *Journal of Social Issues* 43, no. 4 (Winter 1987): 5-71.

9 Morgan, *Deterrence: A Conceptual Analysis*, 28.

10 Lawrence Freedman, "General Deterrence and the Balance of Power," *Review of International Studies* 15, no. 2 (April 1989): 199-210, quote on p. 204, https://doi.org/10.1017/S0260210500113002.

set of any such attempt American power would be employed in stopping it [denial], and, if necessary, would inflict on the Soviet Union injury which the Moscow regime would not wish to suffer [punishment]."[11] Of course, both of these effects are aimed at the mind of an adversary, with denial deterrence, according to Glenn Snyder, presenting "the enemy with a threat which is more easily calculable than punishment deterrence."[12]

The third prominent distinction in the literature is perhaps the most straightforward: direct (or central) deterrence and extended deterrence. Direct deterrence refers to the ability to dissuade an adversary from attacking one's homeland. Extended deterrence is measured by the ability to include other states under that same deterrent umbrella. In the latter case, credibility challenges are prevalent. It is one thing to convince an adversary that one will respond if one's homeland is attacked, whether there be risk of future retaliation and escalation or not. It is quite another to convince an adversary that one will respond if an ally is attacked, thereby assuming retaliatory risk on behalf of others. Much of US effort in the Cold War was in convincing the Soviets of the credibility of the US threat to fight if European Allies were attacked. This was done both through strong statements of commitment and intent that Patrick Morgan called "mortgaging the president's honor."[13] It was also done by forward deploying troops into areas subject to Russian aggression and, in some cases, giving local commanders the authority to respond to an attack. The goal was to remove as much doubt as possible regarding the certainty that an attack on a NATO Ally would engender a response from the US, thereby making extended deterrence credible.

Deterrence in Post-2014 Europe: Theory Meets Practice

While the above review barely scratches the surface of a broad deterrence literature, it does offer a starting point for thinking about deterrence in contemporary Europe. While there was a point when this body of literature looked to be condemned, like the Cold War, to the dustbin of history, the 2014 Russian occupation of Crimea and fostering of instability in eastern Ukraine has once again put deterrence concepts back at the center of European security discussions. It is, therefore, worth considering how NATO efforts at deterrence since 2014 have taken shape and how deterrence theory helps explain these efforts.

In response to what was called the first forcible change of European borders since World War II, the US responded quickly to demonstrate its commitment to NATO territorial sovereignty. The US Operation Atlantic Resolve (OAR) projected a line of small units across NATO's eastern flank as a visible symbol of US resolve.

---

[11] Dean Acheson, *Power and Diplomacy* (New York: Atheneum, 1962), 85.

[12] Glenn H. Snyder, *Deterrence by Denial and Punishment*, Woodrow Wilson School Research Monograph (Princeton University, January 1969), 5.

[13] Patrick M. Morgan, *Deterrence Now* (Cambridge, UK: Cambridge University Press, 2003), 15-16.

Visits by both President Barack Obama and Vice President Joe Biden included an "ironclad" commitment to the security and sovereignty of NATO Allies, and the US Congress appropriated $1B in European Reassurance Initiative (ERI) funds to pay for the enhanced posture of US forces in Europe and begin bringing additional rotational forces from the US.[14] In word and action, Washington responded to Eastern NATO Allies' concern that the moment called for immediate deterrent steps by signaling the US's continued commitment to extended deterrence in Eastern Europe, if only with small numbers of initial forces.

NATO likewise acted collectively to demonstrate resolve in the east. The NATO Readiness Action Plan was developed immediately to implement a range of short-term assurance measures for Eastern Allies and longer-term adaptation measures to improve the deterrence posture of the Alliance. At the 2014 Wales Summit of Heads of State and Government (HOS/G), Allies agreed to a dramatic expansion of the NATO Response Force (NRF), including the development of a Very High Readiness Joint Task Force (VJTF) that could put a brigade's worth of combat power on the ground within 5-7 days of activation. Importantly, the VJTF would be comprised of units from 10 to 15 Allies, signaling a unified response to any aggression that triggered its deployment. We also saw this inclination to staff units with broad representation from across the Alliance in the composition of the NATO Force Integration Units (NFIUs), also agreed at Wales. At the Warsaw Summit two years later, this logic of fielding multi-flagged units to demonstrate NATO unity was extended further, with the advent of enhanced Forward Presence (eFP) in the Alliance's northeast and tailored Forward Presence (tFP) in the southeast.

Thus, like the US's OAR, the VJTF, eFP, and tFP meant that other NATO Allies, too, were signaling a commitment to extended deterrence on the Alliance's eastern flank and, like the US, the combat power of these formations was far from decisive. A 2016 RAND Corporation study stated its findings bluntly, "as currently postured, NATO cannot successfully defend the territory of its most exposed members."[15] This was far from an epiphany. The force posture in the Baltics was particularly problematic and served as a special point of emphasis for the same RAND study. "Across multiple games using a wide range of experts," according to the study's authors David Shlapak and Michael Johnson, "the longest it has taken Russian forces to reach the outskirts of Tallin and Riga is 60 hours."[16] RAND was evaluating the Alliance on its ability to deter by denial in the Baltics, but one might view Allies' efforts, at least through 2016, as working to demonstrate a commitment to extended deterrence through deterrence by *punishment*. That is, broad Allied "skin in the game" would ensure that any act of aggression would

[14] Congressional Research Service, "The European Deterrence Initiative: A Budgetary Overview," *In Focus*, August 8, 2018, https://fas.org/sgp/crs/natsec/IF10946.pdf.

[15] David A. Shlapak and Michael W. Johnson, "Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics" (Arroyo, CA: RAND Corporation, 2016), 1.

[16] Shlapak and Johnson, "Reinforcing Deterrence on NATO's Eastern Flank."

engender a unified Alliance response. If NATO could not prevent an initial decision, forward-deployed NATO troops and initial rapid reinforcement would make a broader conflict and, therefore, NATO retaliation unavoidable.

Meanwhile, both individual Allies and the Alliance have continued to work on longer-term NATO adaptation measures that would allow the Alliance to develop a credible *deterrence by denial* capability. The HOS/G commitment at Wales to move their nations toward spending 2 percent of Gross Domestic Product on defense and spending 20 percent of the defense budget on modernization and equipment was one important step to developing more credible military capabilities.[17] For its part, the US has responded by dramatically increasing defense expenditures earmarked for Europe, increasing ERI spending from $1 Billion in 2015 to $4.8 Billion in 2018, with a request of $6.5 Billion for 2019.[18] In fact, ERI itself was renamed from European Reassurance Initiative to European Deterrence Initiative (EDI) in the 2017 legislation. This money has gone to increase presence of rotational forces, expanded exercises and training, enhanced prepositioning of equipment, improved infrastructure, and the building of partner capacity.

NATO has followed suit, initially allocating $200 Million toward the development of a prepositioning site for US equipment in Poland,[19] and, at the 2018 Brussels Summit, NATO further sharpened its focus on deepening the "NATO bench" and improving readiness in order to be capable of fielding significant combat forces in a shorter period of time. The so-called "four-30s" plan commits Allies to making available 30 troop battalions, 30 squadrons of aircraft, and 30 warships on 30 days notice-to-move.[20] Along with the development of ready units, NATO has also been working on improving intra-European mobility. Ideas like the development of an EU "Schengen Zone-like" collection of countries that commit to expediting military mobility have begun to take shape.[21] Currently, the Alliance is beginning to grapple with the much tougher and more costly task of improving the physical infrastructure required to enable mobility. All of these efforts suggest a transition from an initial focus on establishing the credibility of NATO threats to respond vigorously to any aggression against NATO Allies, ini-

[17] North Atlantic Treaty Organization (NATO), "Wales Summit Declaration," September 5, 2014, para 14, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

[18] Congressional Research Service, "The European Deterrence Initiative."

[19] Department of Defense, "Military Construction Program: FY 2019 Budget," February 2018, 9, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/budget_justification/pdfs/11_NATO_Security_Investment_Program/FY19_NSIP_J-Book_Final.pdf.

[20] North Atlantic Treaty Organization (NATO), "Brussels Summit Declaration," July 11, 2018, para 14, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[21] European Union, External Action Service, "Defence: EU Moves on Military Mobility," March 28, 2018, https://eeas.europa.eu/headquarters/headquarters-Homepage/42226/defence-eu-moves-military-mobility_en.

tially successful or not (deterrence by punishment), to a more calculable ability to deny an aggressor the prospect of an initial, quick victory.

Deterrence Theory as Guide to Future Practice

If we can say, then, that current defense work in Eastern Europe fits well with existing deterrence literature, what might this literature have to say about necessary future work? To answer this question, it is useful to consider some of the reasons past deterrence efforts have failed. Alexander George and Richard Smoke's 1974 typology identifies three patterns for how an adversary might trigger a deterrence failure: the *fait accompli* attempt, the limited probe, and controlled pressure.[22] The differences are determined by the level of risk an aggressor is prepared to take. An attempted *fait accompli* attack comes with the most risk, but it can, according to George and Smoke, be "the most rational" approach if the initiator believes the adversary is unable to prevent the action and does not value the disputed territory enough to warrant the necessary investment of blood and treasure to reverse the initial decision.[23] Observers point to the 2014 annexation of Crimea as the implementation of a *fait accompli* policy.[24] Recognizing the threat posed by such adventurism in the Cold War, Glenn Snyder evaluated NATO defense posture in Europe and concluded that a deterrence by denial force need not be capable of holding out indefinitely or defeating an invader outright, but it did need to be strong enough to convince the Soviets of the Allies' commitment to resist. The operative question, then, in contemporary Eastern Europe is how much and what kind of force is needed to achieve this goal.

A recent report from the Center for European Policy Analysis led by former US Army Europe Commander, Lieutenant General (retired) Ben Hodges, offers some answers to this question, highlighting the requirement for (1) effective early warning, (2) capable national forces, and (3) adequate infrastructure and prepositioned supplies.[25] First, according to the report, early warning in the east is critical to gaining a window of opportunity within which the Alliance can communicate its resolve through additional force deployments, like that of the VJTF and the broader 40,000 troop strong NATO Response Force. Put another way, the more advanced warning NATO has to transition from a general to an immediate deterrence posture, the greater the opportunity for the signaling necessary to eliminate any potential Russian misperception or miscalculation regarding Allies' commitment to collective defense. Second, capable national forces are es-

[22] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, October 1974), 534-547.

[23] George and Smoke, *Deterrence in American Foreign Policy*, 537.

[24] Zdzislaw Sliwa, "Poland: NATO's East Frontline Nation," in *Deterring Russia in Europe: Defence Strategies for Neighbouring States*, ed. Nora Vanaga and Toms Rostoks (Routledge, 2018), 217-236.

[25] Ben Hodges, Janusz Bugajski, and Peter B. Doran, "Securing the Suwałki Corridor: Strategy, Statecraft, Deterrence, and Defense" (Washington, DC: Center for European Policy Analysis, July 2018), 4.

sential to bolstering the east and making eastern NATO Allies an uninviting military target in the first place. The importance of a strong national defense capability is enshrined in NATO's founding treaty, which states in Article 3 that parties to the treaty will, "separately and jointly, by means of continuous and effective self-help and mutual aid, […] maintain and develop their individual and collective capacity to resist armed attack."[26] One especially encouraging example of both of these principles is the potential of strengthened cooperation under the so-called B9+ (Bucharest Cooperation) arrangements, in which the nine eastern Alliance states (Estonia, Latvia, Lithuania, Poland, Czech Republic, Slovakia, Hungary, Romania, and Bulgaria) agree to work collectively on shared challenges such as readiness and interoperability. Third, because it is unrealistic to expect NATO to maintain a forward Cold War-like posture of substantial permanently stationed forces,[27] prepositioned supplies and improved transportation infrastructure are critical to enabling rapid reinforcement. In order to incentivize greater investment here, Lieutenant General (retired) Ben Hodges and his co-authors recommend that NATO develop parameters whereby Allies could count public spending on certain "dual-use" (military and civilian) infrastructure projects toward the agreed NATO 2 percent guideline.[28] While proposals like this do not have the necessary political support at the moment, they do demonstrate a growing awareness of the critical importance of military mobility to preventing any Russian consideration of a *fait accompli* approach. Efforts to demonstrate improved mobility and responsiveness are manifest in an expanded Alliance exercise regime, with the 2017 multinational exercise Saber Guardian providing an important test of the concepts in southeast Europe and the 2018 NATO exercise Trident Juncture doing the same for the north.[29]

As NATO has been making progress on the prevention of potential *fait accompli* failures, it must also keep in mind what George and Smoke refer to as a limited probe approach. In this threat to deterrence, an initiator "creates a controlled crisis in order to clarify the defender's commitments."[30] Rather than an all-out attempt to change the status quo and then challenge the defender to reverse the decision, as in the previous example, an initiator uses a controllable, calculable, and reversible limited probe to test a defender's resolve while at-

[26] "The North Atlantic Treaty," Article 3 (Washington, DC: NATO, April 4, 1949), https://www.nato.int/cps/ie/natohq/official_texts_17120.htm.

[27] In fact, the Alliance continues to abide by the spirit of the NATO-Russia founding act, which commits NATO to collective defense through interoperability and reinforcement, rather than "permanent stationing of substantial combat forces." There is no consensus in the Alliance to change this position. "Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation" (Paris, France: North Atlantic Treaty Organization, May 22, 1997), https://www.nato.int/cps/su/natohq/official_texts_25468.htm.

[28] Hodges, Bugajski, and Doran, "Securing the Suwałki Corridor," 8.

[29] Planning is underway for SABER GUARDIAN 2019, an Allied exercise in southeast Europe of equal or greater scope and scale than the 2017 event.

[30] George and Smoke, *Deterrence in American Foreign Policy*, 540.

tempting to limit the risk of a broader conflict. Such an approach can be especially problematic for an Alliance whose credibility rests on the treaty commitment that an attack on one will be viewed as an attack on all. Ambiguities surrounding the question of what constitutes treaty language like "armed attack" or an Ally's commitment to take "such action as it deems necessary" [31] could turn a limited probe into a poison pill that fractures Alliance unity over how to deal with the transgression.

Here again, communicating 'red-lines' is critical. As Robert Art and Kelly Greenhill argue, "a defender must make crystal clear to any potential attacker what the defender's red lines are by clearly stating its commitment, [… and] by pointing out the costs the challenger will bear should it cross the red lines." [32] Future NATO military exercises and political level crisis management exercises might, therefore, look for creative ways to build limited probe responses into exercise scenarios. Both individually and collectively, Allies might also develop a broader list of military and non-military crisis response measures for different limited probe scenarios. These measures work best when there is broad consensus on what response measures are available and how and when they would be implemented. For this reason, US, NATO, and European Union (EU) cooperation on such work, especially regards non-military measures, would be especially beneficial. Where *a priori* consensus on response measures is not possible, strategic ambiguity will need to be limited through collective statements and clear posturing. The statements and actions of Alliance leadership, especially the US President, are critical in these moments.[33]

The final threat to deterrence, according to George and Smoke, can be seen in patterns of controlled pressure. This approach offers the initiator the least amount of risk and is employed in situations in which the initiator views the defender's commitment as "unequivocal," compared to "pattern one, the initiator's belief is that there is no commitment; in pattern two he believes that there is uncertainty or ambiguity regarding a commitment by the defender." [34] Pattern three, therefore, can be appealing to an adversary who believes he has a particular asymmetric advantage against which the defender cannot offer adequate defense. George and Smoke point to continued Soviet pressure on West Berlin during the Cold War as an attempt to leverage the Soviet geographic advantage in surrounding the historic German capital. The purpose was to gradually erode western commitment to a free West Berlin and exacerbate tensions in the Alliance over the level of commitment NATO should demonstrate on the issue. One sees a similar approach today in Georgia, Ukraine, the Baltics, and Black Sea region, albeit with important differences in tactics across each case.

---

[31] "The North Atlantic Treaty," Article 5.

[32] Art and Greenhill, "Coercion: An Analytic Overview," 12.

[33] Morgan, *Deterrence Now*, 15-16.

[34] George and Smoke, *Deterrence in American Foreign Policy*, 543.

The controlled pressure approach, along with select limited probes, can also be seen in a broad range of activities carried out below the level of conflict. These so-called "gray zone" or "hybrid" approaches are generally characterized by "activity that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war."[35] This makes the strategy ideal for controlled pressure efforts to defeat deterrence. It can be waged in a traditional geographic context through proxies, as in Eastern Ukraine, or through economic coercion, information warfare, sabotage, and, especially, cyber-attacks. Moreover, as traditional NATO deterrence efforts strengthen, this controlled pressure approach to undermining deterrence through gray zone efforts becomes more appealing to those wishing to change the status quo while avoiding open conflict. It is a new front in a more classic deterrence stand-off that poses one of the more difficult challenges for contemporary deterrence.

The Grey-Zone and the Stability / Instability Paradox

With new technologies opening up new opportunities for a controlled-pressure strategy to defeat Alliance deterrence efforts, the Alliance has witnessed the emergence of what might be termed a "stability-instability paradox." The term was first coined in the 1960s to describe the way in which nuclear weapons constrained great power war, creating a level of overt stability even as adversarial states waged a low level but frenetic campaign of influence and proxy wars. A similar dynamic can be seen in the way strengthened Alliance conventional deterrence measures backed by extended nuclear deterrence have led adversaries to look for ever more controllable and calculable ways to exert pressure on deterrence regimes. Put another way, while NATO conventional deterrence efforts appear to be settling Eastern Europe into a general deterrence state of affairs, grey-zone probes, assaults, and campaigns continue to call for more crisis management-like responses, including actions to bolster immediate deterrence. Though these basic dynamics can be seen in examples across different hybrid spheres of action, cyber and the information sphere are several areas worth highlighting.

"The biggest problem in cyber," according to Estonia's former President Toomas Ilves, "remains deterrence. We have been talking about the need to deal with it within NATO for years now."[36] Indeed, Richard Clarke and Robert Knake go so far as to argue that deterrence theory simply does not transfer very well

[35] Hal Brands, "Paradoxes of the Gray Zone," *Social Science Research Network Electronic Journal* (January 2016), 1, http://dx.doi.org/10.2139/ssrn.2737593.

[36] Quoted in Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, quote on p. 44, https://doi.org/10.1162/ISEC_a_00266.

to the cyber domain,[37] and, where there has been theory transfer, the focus has generally been on deterrence by denial through network defenses and more resilient systems. In fact, the former US Deputy Secretary Defense William Lynn offered this view in arguing that "deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation."[38] This has also been the primary approach by NATO, initially focusing on the protection of NATO networks and enhancing resilience through education, mutual assistance, and cyber rapid reaction teams.[39] However, at Warsaw, NATO adopted cyberspace as a domain of operations, and the 2018 Brussels Summit resulted in an agreement to establish a Cyberspace Operations Center and to "continue to work together to develop measures which would enable us to impose costs on those who harm us."[40] Thus, despite some challenges, NATO has continued to adapt deterrence concepts to the emerging cyber domain of operations, evolving from a focus on defending NATO networks to assisting Allies with resilience and, eventually, a recognition of the need for a deterrence by punishment capability.

Allies' efforts have also begun to signal a more holistic approach to the application of deterrence concepts in cyber. According to Zdzislaw Sliwa, Poland's publication of its 2015 "Information Security Doctrine of the Republic of Poland" was an effort to establish a deterrence by denial posture.[41] Nevertheless, the document also highlights the requirement for "pursuing active cyberdefence, including offensive actions in cyberspace, and maintaining readiness for cyberwar."[42] Owing to a broad 2007 Russian cyber-attack, Estonia is perhaps the most forward-leaning Ally on the question of cyber. As a result, the 2017 defense development plan commits the country to the creation of "a national Cyber Command to develop both defensive and offensive cyber capabilities."[43] Finally, despite Deputy Defense Secretary Lynn's earlier comments, the United States' most recent 2018 cyber strategy offers a similar recognition that deterrence in the cyber domain requires both denial and punishment capabilities, arguing that

---

[37] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 189.

[38] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108.

[39] North Atlantic Treaty Organization, "Cyber Defence," July 16, 2018, www.nato.int/cps/en/natohq/topics_78170.htm.

[40] North Atlantic Treaty Organization, "Brussels Summit Declaration," July 12, 2018, para 20, https://www.nato.int/cps/ic/natohq/official_texts_156624.htm.

[41] Sliwa, "Poland: NATO's East Frontline Nation."

[42] National Security Bureau (Biuro Bezpieczenstwa Narodowego), "Cybersecurity Doctrine of the Republic of Poland," January 2015, accessed February 4, 2018, http://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.

[43] Henrik Praks, "Estonia's Approach to Deterrence," in *Deterring Russia in Europe: Defence Strategies for Neighboring States*, ed. Nora Vanaga and Toms Rostoks (New Yourk: Routledge), 217-235.

"activity that is contrary to the responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means."[44] This latter point bears highlighting. Deterrence by punishment in the cyber domain may rely on a symmetric cyber response, but it might also include other asymmetric retaliatory measures, as with the imposition of US economic sanctions on Russia in response to meddling in the 2016 US elections. Achieving effective cyber deterrence will require Allies to continue exploring how both symmetric and asymmetric response options might best be employed and signaled ahead of time.

Being especially vulnerable, Eastern European states should continue to explore how they might adapt their own cyber strategies and deepen cooperation with other Allies in the cyber domain. Both the Bulgarian and Slovenian cyber strategies were developed in 2016, while Hungary and Romania's strategies date from 2013, before the 2016 NATO Cyber Defense Pledge. The establishment of cyber defense as an Alliance domain of operations, the affirmation that cyber defense is a part of NATO's collective defense core task, and the creation of a NATO Cyberspace Operations Center all speak to the expansion of concern and cooperation in this area. Ideas, like those put forward by the Atlantic Council of Bulgaria, to establish a cyber and hybrid threats response center should be considered as ways to foster continued interoperability and coordination.

A second hybrid challenge for NATO can be seen in the way Moscow has targeted media markets to influence messaging toward Russian political and economic interests. Findings from a recent Center for the Study of Democracy report describe pro-Russian oligarchic networks that exert broad control over Black Sea media markets either through outright ownership or the cultivation of other forms of economic dependency.[45] This has resulted in more-or-less consistent Moscow-directed misinformation and message spin in the impacted countries. The case of Bulgaria is especially enlightening. Having made foreign media investment illegal, national media markets were rapidly dominated by a handful of local actors who serve as a vehicle for illicit external funds. Rather than preventing outside influence, the measure ensured that foreign influence would be furtive and less-transparent, facing little market competition.

As these and other hybrid threats pose an ever greater challenge, methods of dealing with them have largely followed a deterrence by denial path, including the strengthening of political, economic, and societal resilience. Indeed, the Center for the Study of Democracy calls for a variety of EU sponsored measures to bolster Black Sea area media resilience, like programs to improve journalistic standards and prevent so-called media capture by malign external actors. Simi-

[44] "National Cyber Strategy of the United States of America," (Washington, DC: The White House, September 2018), 3, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[45] Center for the Study of Democracy (CSD), *Russian Influence in the Media Sectors of the Black Sea Countries: Tools, Narratives, and Policy Options for Building Resilience* (Sofia, Bulgaria: Black Sea Trust for Regional Cooperation and the German Marshall Fund, 2018).

larly, Radio Free Europe returned to both Romania and Bulgaria in December 2018 as a result of growing concern about the health of a free press in the region.[46] While these measures are sorely needed, deterrence by punishment approaches might also be considered. Such disincentives might include aggressive legal action and sanctions for individuals or groups that violate national laws. Here again, a cyber and hybrid threats response center like that proposed by Bulgaria's Atlantic Council could make important contributions to the effort and would have the advantage of plugging into a community of interest doing similar work across Europe.[47]

Conclusions

Though deterrence theory is certainly no panacea for either the conventional or hybrid threats that face Eastern Europe, a consideration of some of the deterrence theory's key principles can help organize thinking and identify additional questions worth considering. One way of understanding Alliance efforts since 2014 has been to address the more immediate threats to deterrence first, preventing the *fait accompli* attack and drawing red-lines against limited probe efforts. This was done initially by establishing the expectation that rapid reinforcement and forward deployment would guarantee Alliance retaliation, deterring further adventurism through the prospect of punishment. The great challenge in this approach was in making the likelihood of punishment and the US commitment to extended deterrence credible. This effort has since been augmented by more sustained efforts to field capabilities that can oppose local, geographic Russian force advantages through stronger national forces, early warning, rapid mobility, and prepositioned equipment. This move toward deterrence by denial requires greater pre-crisis preparation of Eastern European defenses but can be more reliable in that it is easier for an adversary to calculate the risk aggression would entail.[48]

Nevertheless, even as these efforts continue to mature, controlled pressure challenges to NATO deterrence means that Alliance unity and resolve are under persistent assault. Individually, Allies are alive to the danger, and, collectively, the Alliance is coming to terms with the role NATO might play in addressing grey-zone threats. What are the symmetric and asymmetric capabilities, response options, and crisis response measures that should be available? Do such capabilities belong in the NATO Defense Planning Process? How to ensure complementarity between individual Allies, NATO, and the EU? What is the role of NATO, including

[46] Eugen Tomiuc, Eugen Tomiuc "RFE/RL to Launch News Services in Romania, Bulgaria," *RadioFreeEurope/RadioLiberty*, July 19, 2018, https://www.rferl.org/a/rfe-rl-to-launch-news-services-in-romania-bulgaria/29376248.html.

[47] The Hybrid Center of Excellence in Finland and Cyber Center of Excellence in Estonia are two important examples for where multinational cooperation might be leveraged to advance national work.

[48] Snyder, *Deterrence by Denial and Punishment*, 5.

Article 4 consultations, in bringing visibility to controlled pressure tactics? These are but a few of the questions for future work.

While all of this has to do with the one big idea of the hedgehog, deterrence, it also suggests that the application of deterrence in the contemporary security environment requires some of the more wide-ranging and innovative approaches of the fox. To borrow a phrase from another NATO playbook, the application of 21st Century deterrence will require a *comprehensive approach*. This includes a comprehensive approach to resilience (deterrence by denial) and a comprehensive approach to imposing proportional costs on aggressors (deterrence by punishment).[49] A workable strategy to do both would better enable Allies to deter on both ends of the conflict to the competition spectrum. This will demand both persistence and adaptiveness to accomplish enduring goals with new tools to employ against varied threats. It will require the instincts of both the hedgehog and the fox.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Colonel **Darrell Driver**, U.S. Army, is an Associate Professor and the Director of European Studies at the U.S. Army War College. His previous positions have included Director of NATO Support for U.S. European Command, Defense Policy Advisor to the U.S. Mission to NATO, Senior Fellow and Faculty Member at the George C. Marshall European Center for Security Studies, and Assistant Professor of Political Science at the U.S. Military Academy. He is the author of a number of articles and book chapters on subjects related to European security and civil-military relations. He holds a PhD (2006) in Political Science from Syracuse University. *E-mail*: darrell.w.driver.mil@mail.mil.

[49] In fact, Chris Kremidas Courtney describes hybrid warfare as the "comprehensive approach in the offense." For more on this, see Chris Kremidas Courtney, "Hybrid Warfare: The Comprehensive Approach in the Offense," *Friends of Europe: Europe's World*, December 2018.

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

V. Shalamanov, P. Anastasov & G. Tsvetkov
Connections QJ 18, no. 1-2 (2019): 25-42
https://doi.org/10.11610/Connections.18.1-2.02

Research Article

Deterrence and Defense at the Eastern Flank of NATO and the EU: Readiness and Interoperability in the Context of Forward Presence

Velizar Shalamanov, [1] ***Pavel Anastasov,*** [2] ***and Georgi Tsvetkov*** [3]

[1] *Institute of ICT, Bulgarian Academy of Sciences, http://www.iict.bas.bg/EN*

[2] *Political Affairs and Security Policy Division, NATO International Staff*

[3] *"G. S. Rakovski" National Defence College, Sofia, https://rndc.bg/en/*

Abstract: This article reflects the discussions during a September 2018 conference in Sofia, sponsored by the NATO Public Diplomacy Division. Its focus is on the defense and deterrence posture of NATO and the European Union in Eastern Europe. Special attention is given to the development of the Bucharest Initiative (B9) and its influence on the Western Balkans and Black Sea Region. The authors propose a Program for Readiness and Interoperability, oriented to the C4ISR area. This is based on the defense posture and in the context of the developments in NATO and the European Union for improved readiness and interoperability with partners that, together with enhanced cooperation in education and training for the defined B9+ region, will act as instruments to implement this cooperation and improve the deterrence and defense capability on the Eastern Flank of NATO and the EU, while at the same time strengthening resilience to hybrid threats.

Keywords: NATO, European Union, defense, deterrence, readiness, interoperability, cooperation, Eastern flank, Balkans, Black Sea region, resilience.

Creative Commons BY-NC-SA 4.0

NATO Presence in Eastern Europe after the Changes of 1989 [1]

The elaboration in this article is based on developments of multinational formations in Central and Eastern Europe (CEE)/South Eastern Europe (SEE), improving their interoperability and readiness through multinational projects, especially in the area of Communications and Information (C&I), and adequate education and training, including exercises. Further research is proposed in a multinational format to define programs for the readiness and interoperability of multinational formations in CEE/SEE.

After the changes in 1989, NATO was seriously involved in Eastern Europe, and a visible presence of military formations began in 1995 with the responsibility to the United Nations (UN) for carrying out the Dayton Peace Accords. This agreement was signed on November 22, 1995 by the presidents of Bosnia, Croatia, and Serbia, on behalf of Serbia and the Bosnian Serb Republic. The actual signing took place in Paris on December 14, 1995. The accords had three major goals: the ending of hostilities, the authorization of military and civilian programs, and the establishment of a central Bosnian government while excluding war criminals from taking part in the running of the government. The first NATO-led multinational force (IFOR) was established to implement the military Annexes of *The General Framework Agreement for Peace (GFAP) in Bosnia and Herzegovina*.

IFOR relieved the UN peacekeeping force (UNPROFOR), which had originally arrived in 1992, and the transfer of authority was agreed upon in Security Council Resolution 1031. Almost 60,000 NATO soldiers, in addition to forces from non-NATO nations, were deployed to Bosnia. Operation Decisive Endeavor (SACEUR OPLAN 40105) that began on December 6, 1995, was a subcomponent of Joint Endeavor.

The next large multinational presence was SFOR which was established by Security Council Resolution 1088 on December 12, 1996, to succeed IFOR. Troop levels were reduced to approximately 12,000 by the close of 2002, and to approximately 7,000 by the close of 2004 when, at the Istanbul Summit of NATO, the end of the mission was announced.

Operation *Althea*, formally European Union Force (EUFOR) in Bosnia and Herzegovina, is the successor to SFOR/IFOR. The transition from SFOR to EUFOR was largely a change of name and commanders: 80% of the troops remained in place. Formally, it replaced SFOR on December 2, 2004.

KFOR was the next large multinational deployment in Eastern Europe after NATO's first actual combat operation in Europe.[2] Following the adoption of UN Security Council Resolution 1244, troops entered Kosovo on June 11, 1999. At the time, Kosovo was facing a grave humanitarian crisis with nearly one million

[1] This section draws extensively on information posted on the NATO web site, https://www.nato.int, and the English version of Wikipedia.

[2] Gen. Wesley K. Clark, *Waging Modern War: Bosnia, Kosovo and the Future of Combat* (New York: Public Affairs, 2001).

people displaced as refugees. At its height, KFOR troops numbered 50,000 and came from 39 different NATO and non-NATO nations.

KFOR, during the years, has gradually transferred responsibilities to the Kosovo Security Forces and other local authorities and, as of May 23, 2016, consisted of 4,600 troops. Recently, the Kosovo Force in Pristina (2018) consisted of: Headquarters Support Group (HSG), in Pristina; Multinational Specialized Unit (MSU), in Pristina (a Military Police regiment composed entirely of Italian Carabinieri); Multinational Battle Group-East (MNBG-E) at Camp Bondsteel near Ferizaj (a US Army force supported by Hungary, Poland, Romania, and Turkey); Multinational Battle Group-West (MMBG-W) at Camp Villaggio Italia near Peć (an Italian Army force supported by Austria, Moldova, and Slovenia); Joint Logistics Support Group (JLSG) in Pristina (Logistics and engineering support); KFOR Tactical Reserve Battalion (KTRBN) at Camp Novo Selo (Composed entirely of Hungarian Army troops); Joint Regional Detachment – North (JRD-N) at Camp Novo Selo (local non-kinetic liaison and monitoring); Joint Regional Detachment-Centre (JRD-C) in Pristina (local non-kinetic liaison and monitoring); Joint Regional Detachment – South (JRD-S) in Prizren (Local non-kinetic liaison and monitoring).

Experience gained in the Balkans was essential in defining the crisis management and the use of multinational formations down to the tactical level. Acting outside of Europe, ISAF was a multinational force of critical importance for the development of the concept of interoperability, especially with the introduction of the Afghanistan Mission Network (AMN) as an operational tool.[3]

The next large operation—Unified Protector—was a challenge while at the same time an opportunity to test readiness and interoperability in Air and Maritime domains.[4] The crisis management challenge from an operational perspective was addressed through a number of different initiatives that included a Complex Crisis Operations Management Center (CCOMC) to provide situational awareness and support further planning with the available ready and interoperable forces, which were, as a rule, multinational formations.[5]

The transition from crisis management was most visible at the Wales Summit in 2014 when the NATO allies agreed to implement the Readiness Action Plan (RAP) in order to respond swiftly to the fundamental changes in the security environment on NATO's Eastern borders.

Building on the RAP, the Allies took further decisions at the Warsaw Summit in 2016 to strengthen NATO's deterrence and defense posture and to contribute to projecting stability and strengthening security outside of Alliance territory. Together, these decisions were the biggest reinforcement of Alliance collective defense in a generation. Combined with the forces and capabilities required for

[3] Gen. Stanley McChrystal, *My Share of the Task: A Memoir* (New York: Penguin Publishing Group, 2013).

[4] Rob Weighill and Florence Caub*, The Cauldron: NATO's Campaign in Libya* (London: Hurst Publishers, 2018).

[5] James Stavridis, *The Accidental Admiral: A Sailor Takes Command at NATO* (Annapolis, Maryland: Naval Institute Press, October 2014).

rapid reinforcement by follow-on forces, these measures will enhance the security of all Allies and ensure the protection of Alliance territory, populations, airspace, and sea lines of communication, including across the Atlantic, against threats from wherever they arise.

NATO's enhanced forward presence is defensive, proportionate, and in line with international commitments. It represents a significant commitment by Allies and is a tangible reminder that an attack on one is an attack on all.

Fully deployed in June 2017, NATO's enhanced forward presence comprises multinational forces provided by framework nations and other contributing Allies on a voluntary, fully sustainable, and rotational basis. They are based on four rotational, battalion-size battlegroups that operate in concert with national home defense forces and are present at all times in the host countries. Canada, Germany, the United Kingdom, and the United States are the framework nations for this robust multinational presence in Latvia, Lithuania, Estonia, and Poland, respectively.

Other Allies have confirmed contributions to these forces: Albania, the Czech Republic, Italy, Poland, Slovakia, Slovenia, and Spain contribute to the Canadian-led battlegroup in Latvia; Belgium, the Czech Republic, Iceland, Luxembourg, the Netherlands, and Norway have joined the German-led battlegroup in Lithuania; Denmark and Iceland contribute to the UK-led battlegroup in Estonia; and Croatia, Romania, and the United Kingdom have joined the US-led battlegroup in Poland. These enhanced forward presence forces are complemented by the necessary logistics and infrastructure to support pre-positioning and to facilitate rapid reinforcement. The four battlegroups are under NATO command through the Multinational Corps Northeast Headquarters in Szczecin, Poland. These four battlegroups' training and preparation activities are coordinated and supervised by the Multinational Division Northeast Headquarters (MND-NE) in Elblag, Poland.

At the 2016 Summit in Warsaw, the Allies also agreed to develop a tailored forward presence in the south-eastern part of Alliance territory. On land, this presence is built around the Romanian-led multinational brigade in Craiova. In the air, several Allies have reinforced Romanian and Bulgarian efforts to protect NATO airspace. This means more NATO forces and more exercises and training under the Headquarters Multinational Division Southeast (in Romania), which became fully operational in June 2017. This tailored forward presence contributes to the Alliance's strengthened deterrence and defense posture and to its situational awareness, interoperability, and responsiveness.

All these changes are in response to Russia's aggressive behavior since 2008, but the turning point was really the annexation of Crimea and the aggressive actions in Eastern Ukraine, together with the development of the hybrid warfare concept and its implementation. It means that to the East NATO faces the Rus-

sian hybrid challenge,[6] but, at the same time, a very real Russian conventional challenge.[7]

NATO's rapid reinforcement strategy also ensures that forward presence forces will, if necessary, be reinforced by NATO's Very High Readiness Joint Task Force, the broader NATO Response Force, the Allies' additional high readiness forces and NATO's heavier follow-on forces. NATO is also developing several additional measures to increase its presence in the Black Sea region. Specific measures for a strengthened NATO maritime and air presence in the region are being implemented, with several Allies contributing forces and capabilities. Though the forward presence is mostly focused in North-Eastern Europe, the geostrategic importance of the Black Sea is growing,[8] especially for Russia after the annexation of Crimea, and as a result, there is a visible confrontation between Russia and NATO[9] in the region.

Based on this short review of the development of multinational forces for crisis management as well as for deterrence and defense, the remainder of the article explores the potential in CEE after NATO's Brussels Summit (2018) with related opportunities to improve readiness and interoperability through multinational communications and information projects and adequate training.

The Deterrent Potential of the Alliance in Its Eastern Area of Responsibility – the Way Ahead

The Alliance's Eastern area of responsibility and the Black Sea Region continues to be one of the most dynamic regions with some of the greatest security challenges. They all stem from Russia's aggressive posture in the East, the South of Europe, and the Western Balkans. After the Brussels Summit, at the NATO sponsored international conference in Sofia, Bulgaria in 2018, the special panel on deterrence and defense posture in Eastern Europe agreed that out of the three main tasks of collective defense, crisis management, and cooperative security, collective defense remains the key focus with steady and fast evolution through

---

[6] Franklin D. Kramer and Lauren M. Speranza, "Meeting the Russian Hybrid Challenge: A Comprehensive Strategic Framework" (Washington, DC: Atlantic Council, Brent Scowcroft Center on International Security, May 2017), https://www.atlanticcouncil.org/in-depth-research-reports/report/meeting-the-russian-hybrid-challenge.

[7] Franklin D. Kramer and Hans Binnendijk, "Meeting the Russian Conventional Challenge: Effective Deterrence by Prompt Reinforcement" (Washington, DC: Atlantic Council, Brent Scowcroft Center on International Security, February 2018), www.atlanticcouncil.org/in-depth-research-reports/report/meeting-the-russian-conventional-challenge.

[8] Bouris Toucas, The Geostrategic Importance of the Black Sea Region: A Brief History, Center for Strategic and International Studies (CSIS), February 2, 2017, www.csis.org/analysis/geostrategic-importance-black-sea-region-brief-history.

[9] Boris Toucas, NATO and Russia in the Black Sea: A New Confrontation? Center for Strategic and International Studies (CSIS), March 6, 2017, available at https://www.csis.org/analysis/nato-and-russia-black-sea-new-confrontation.

the summits in Wales, Warsaw, and Brussels. This evolution was described as moving from a posture of deterrence by punishment to one of deterrence by denial. New decisions raised at the Brussels Summit, such as the NATO Readiness Initiative, but also the current development of forward presence measures together with the US European Defense Initiative (EDI), have reaffirmed the steadfast commitment of NATO to collective defense and of the US to European defense.

NATO Eastern flank representatives at the conference gave priority to further development of the deterrence by denial scenario with a focus on the role of the Bucharest 9 (B9) format of cooperation to become the voice of CEE.[10] The Alliance must continue to focus its efforts on improving expanded military capabilities in order to demonstrate a credible ability to oppose aggression from the first instance. The focus within the NATO core task should be on advanced planning, military mobility within the Alliance, and initiatives for readiness with forward presence and improved interoperability in the multinational environment on the tactical level. In greater detail, this deterrent capability requires (1) improved early warning systems to allow the Alliance more time to react, (2) credible national forces capable of waging initial defense, and (3) enhanced mobility and pre-positioned equipment to enable that broad Alliance response.

One important element is the firm understanding that NATO adaptation and European Union (EU) developments in the defense area should be fully synchronized. The advantages of the EU defense industrial complex and developing defense research programs, the tools available to the European External Action Service, and the development of the PESCO projects should all be in line with NATO developments and are complementary to one another while making both NATO and EU stronger and safer. The European Union should continue making the best use of NATO defense policy and planning methodology. Good coordination between NATO and the EU headline goal process and capability development plan is a must.

Bulgaria, Romania, and Turkey are the main stakeholders in the development and implementation of the current NATO Tailored Forward Presence measures. These measures build up the Alliance deterrence and defense posture in the Black Sea Region and have to be fully synchronized with the security of the North East/Baltic Region of Eastern Europe (Baltic States, Visegrad Group) linked with the Western Balkans and Adriatic Sea. The multinational brigade in Craiova, with Romania as a framework nation, is the main element of the land component. In the air domain, the Allies are reinforcing the efforts of Romania and Bulgaria for air policing. In the maritime domain, standing NATO maritime forces are present with more ships and more naval exercises in the region. A Black Sea Functional

[10] Marcin Terlikowski, with Veronika Jóźwiak, Łukasz Ogrodnik, Jakub Pieńkowski, and Kinga Raś, "The Bucharest 9: Delivering on the Promise to Become the Voice of the Eastern Flank," *PISM Policy Paper* no. 4 (164) (Warsaw: Polish Institute of International Affairs, 2018), accessed October 29, 2018, http://www.pism.pl/Publications/PISM-Policy-Paper-no-164.

Centre has been established within the NATO Maritime Command. A new enhanced training initiative aims to bring more coherence in all training efforts in the region. Generally, all tailored measures should ensure readiness and interoperability.

Seen as strictly military-technical issues prior to the Wales Summit, now readiness and interoperability are becoming the key criteria for the effectiveness of NATO's adaptation to the Russian conventional challenge. And this is where the Allies will need to show resolve since both readiness and interoperability cost a lot. The need for being innovative and thinking of cost-effective options should be explored and developed in order to demonstrate credible deterrence. This includes more rotations for exercises, cross-border air training (which might be based on the NORDEFCO model), a maritime presence (on both Baltic and Black Seas), and more permanent stationing.

Bulgaria must work to ensure a real and continuous presence of Allied forces on its territory by hosting land, air, and naval components of the NATO Forward Presence such as hosting:

- a coordination element of the Allied Maritime Command in Varna, connected with the NATO Force Integration Units (NFIUs) in Sofia and Bucharest;
- a multinational Air Force fighter squadron on a rotational basis, in a Bulgarian military airbase (especially during the period of acquiring a new fighter and potentially accelerating the outgoing of the MiG-29) that should carry out joint allied air policing of the Bulgarian airspace, potentially to cover the airspace of North Macedonia after finalizing the accession process (in cooperation with Greece and other Allies);
- a multinational mechanized brigade or a multinational Special Operations brigade, with Bulgaria being the framework nation.

As an expression of solidarity and cohesion along the whole Eastern Flank, Bulgaria must join one of the established four NATO multinational battlegroups in the Baltic states and Poland.

The new Readiness Initiative, agreed at the Brussels Summit, should improve NATO's ability to mobilize and deploy larger reinforcements and hence enhance deterrence and defense on the Alliance's Eastern Flank. The initiative should ensure that more high-quality, combat-capable national forces at high readiness can be made available to NATO. From within the overall pool of forces, the Allies will offer an additional 30 major naval combatants, 30 heavy or medium maneuver battalions, and 30 kinetic air squadrons, with enabling forces, at no more than 30 days' readiness. They will be organized and trained as elements of larger combat formations in support of NATO's overall deterrence and defense posture. As stated in the Summit Communique, the Readiness Initiative will further enhance the Alliance's rapid response capability, either for the reinforcement of Allies in support of deterrence or collective defense, including for high-intensity warfighting, or for rapid military crisis intervention, if required. It will also pro-

mote the importance of effective combined arms and joint operations. Being the logical evolution after the Wales Summit, the Readiness Action Plan, and the Warsaw Summit focus on Forward Presence, this new initiative, as ambitious and important as it might be, could face a lot of challenges in its implementation.

A number of areas will need special attention because increasing and maintaining forces' readiness involves high costs. The 30 days target will also need to be further discussed, given Russia's regional superiority in land forces. For countries like Bulgaria, in addition to the challenges of providing trained and equipped units, the ability to provide host nation support and mobility needs to be considered urgently by the national authorities. Bearing in mind that the acquisition of the new NATO interoperable fighters and ships in Bulgaria was postponed in 2014, the most obvious contribution would be a mechanized battalion. Working closely with Albania, Montenegro and, soon, North Macedonia, it will be possible to contribute to the Readiness Initiative with regional multinational battalions dedicated to NATO that will facilitate interoperability and readiness.

It is important, also, to consider the efforts of both NATO and the EU to improve military mobility by land, air, and sea, their tackling of the related physical barriers such as deficiencies in infrastructure and its incompatibility with military requirements, as well as the shortages in means of transportation. In addition, the need for tackling procedural obstacles, such as the time for national permission for a border crossing by forces and equipment, must also be addressed.

The Brussels Summit reconfirmed the commitment to the Defense investment pledge of the 2014 Wales Summit. Fair burden-sharing underpins the Alliance's cohesion, solidarity, credibility, and the ability to fulfill Article 3 and Article 5 commitments. Allies have started to increase the amount they spend on defense in real terms and two-thirds of the Allies have national plans in place to spend 2% of their Gross Domestic Product on defense by 2024. More than half of them are allocating more than 20% of their defense expenditures on major equipment, including related research and development, and, according to their national plans, 24 Allies will meet the 20% guideline by 2024.

Bulgaria must review and adapt its government plans to commit to reaching the level of defense spending of 2% of the GDP in 2020, instead of in 2024. They must also plan to attain a level of spending on new capabilities and research of at least 20% of the total defense spending (and potentially to identify a model for increased defense spending above these levels during the early stages of rearmament in order to accelerate the replacement of old, non-interoperable and often risky-to-operate Soviet equipment). This should be in line with reaching an agreement on the setting of a deadline for the termination of member states' dependence on the Russian Federation for the maintenance of major weapon systems and equipment, including, by way of enhanced cooperation, in the framework of NATO and the EU.

An additional national measure to be considered here is the establishment of an Armaments Acquisition Agency that must be created with clearly defined roles, responsibilities, and tasks, in accordance with the principles of democracy

and good governance. This should include project management mechanisms and close coordination with NATO and European armaments and acquisition agencies. Within its mandate, it must work towards finding synergies within its joint acquisition and maintenance capabilities with NATO Allies/EU Member states in the Western Balkans, the Black Sea Region and beyond.

Further, as Laura Brent pointed out in a recent article in NATO Review, "Cyber threats to the security of the Alliance are becoming more frequent, coercive, complex, and destructive." [11] Cyber defense is part of NATO's core task of collective defense. Bulgaria must be able to operate as effectively in cyberspace as it does in the air, on land, and at sea to strengthen and support the Alliance's overall deterrence and defense posture. Therefore, Bilgaria can provide an important contributin toe deterrence and defense by delivering a strong national cyber defense through the full implementation of the Cyber Defense Pledge, which is central to enhancing cyber resilience and raising the costs of a cyber-attack.

A suggested measure for Bulgaria is creating a cyber and hybrid threats response center under the Ministry of Defense with tasks to investigate, analyze, and then coordinate and implement measures to counter cyber and hybrid threats. This center must be linked with NATO HQ capabilities for early warning as well as with the relevant Centers of Excellence in the NATO and EU framework. The development of new regulations in the EU on the set-up of a European cybersecurity industrial, technology and research competence with a network of national coordination centers calls for close coordination with defense area developments on a national level and respectively with NATO.

Together with good NATO/EU cooperation, regional cooperation is a critical dimension of success. The group of nations most concerned with the deterrence and defense of NATO's Eastern Flank could be defined as Bucharest 9+/B9+ (the Eastern Flank Allies which are Poland, the three Baltic States, Hungary, Czech Republic, Slovakia, Romania, Bulgaria, but also Albania, Montenegro, and Croatia, with North Macedonia as a future member state). This format could actively engage with key NATO partners such as Georgia and Ukraine. These two partners have continuously stated that they welcome Alliance efforts to provide a credible defense on its Eastern Flank and to continue its commitment to maintaining stability in the wider Black Sea Region. A good example of a similar relationship is between Sweden and Finland (EU, but not NATO members) who are actively engaged in projecting stability in the Baltic Sea Region.

Following the best practices from NORDEFCO and BENELUX, project-based cooperation in the B9 format must continue to be developed. The initiation of a flagship Program for Readiness and Interoperability (PRI) in this context, as defined below, could be the first step for change. There is a great potential for integration through exercises and real operations for a number of national and multinational formations in the region. Following the example of the "NATO First

[11] Laura Brent, "NATO's Role in Cyberspace," *NATO Review*, 12 February 2019, https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

Solution" used for NATO Force Structure HQs, PRI could be fully supported by the NATO Communications and Information Agency (NCIA) and the NATO Support and Procurement Agency (NSPA). Regional projects for air and maritime surveillance are potential pilot projects to follow and a joint review of other procurement/ logistics in the B9+ format could provide a solid base for the portfolio of multinational projects to procure equipment or at least to have regional maintenance and overhaul systems with NSPA support.

The Development of Interoperability and Readiness Initiatives in NATO

The roots of change began at the Prague Summit in November 2002, when NATO recognized that the transformation of the military based upon the Information Age principles was essential. A course of transformation following the concept of *NATO Network-Enabled Capabilities* (NNEC) was then pursued. All operations in the Balkans[12] (Bosnia and Herzegovina, Kosovo), with a presence in Albania and Macedonia as well, provided so much experience that it provoked a transformational endeavor in NATO with the turning point based on ISAF[13] and OUP.[14] Recently the implementation of RAP and the new Readiness Initiative are providing further impetus to these efforts.

A good example, in 2003, was how nine NATO nations (Canada, France, Germany, Italy, the Netherlands, Norway, Spain, the United Kingdom, and the United States) arranged to fund a feasibility study on NNEC. This study was assigned to the NATO C3 Agency (NC3A), and later, the ACT launched an awareness campaign to promote the NNEC concept based on the results of the study. At the same time, the NNEC Program office was established in NC3A to manage all NNEC related common funded projects. Achieving full collaboration and full coherence between the various projects of NATO and NATO Nations is the long-term goal, so in 2009 the Agency formed a new sponsor account "NATO and Nations" to support the implementation of the C4ISR projects outside the NATO Command structure, related to interoperability in the C&I domain.

The NNEC program aimed at producing a federation of capabilities at all levels, military (strategic to tactical) and civilian, through an information infrastructure and, at the same time, following the vision of "Share to Win," started work on a culture change for the people involved. Information sharing is the precondition for better situational awareness and faster decision-making that improves collaboration between nations which, ultimately, saves lives and resources. The *information infrastructure* is the supporting base that enables collaboration and information sharing amongst users and reduces the decision-cycle time. This

[12] Clark, *Waging Modern War*.

[13] McChrystal, *My Share of the Task*.

[14] Weighill and Caub, *The Cauldron*.

leads to *information superiority*,[15] which is the ability to get the right information to the right people at the right time.

In 2009, the NATO Consultation, Command and Control Agency (NC3A) recognized the growing demand to support nations in addition to NATO common funded C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) programs in the development of modern, interoperable and secure C4ISR capabilities. So, the Agency proposed on November 11, 2009, the NATO Comprehensive Approach[16] to C4ISR to the NC3 Board for notation.

The C4ISR/Cyber domain in the context of *Federated Mission Networking* (FMN) plays a central role in force integration. In order to accelerate the development in this area, especially for Eastern European NATO members and partners in NC3A (now NCIA), the establishment of a C4ISR Integration Fund[17] was proposed in 2010. The implementation of this model started in 2014 with the *C4 Trust Fund* for Ukraine led by Canada, UK, and Germany and supported by NCIA.

To a great extent, the Agency Reform initiative for the C4ISR area, approved at the Lisbon Summit in 2010, was endorsing the NATO Comprehensive Approach to C4ISR. It provided support for the whole security sector, going outside the defense establishment to include other partners. It also covered the whole life cycle of C4ISR capabilities from requirements definition to deployment and even decommissioning. Furthermore, it used all available funding sources from common funding through multinational and trust fund-based funding to individual nations funding.

In the C4ISR area, this comprehensive approach provided a basis for "Smart Defense" for capability development and service provision by modeling this area even before its announcement as a flagship NATO initiative at the Chicago Summit in May 2012. There, NATO leaders agreed to embrace Smart Defense[18] to ensure that the Alliance could develop, acquire and maintain the capabilities required to achieve the goals of "NATO Forces 2020" of modern, tightly connected forces that are properly equipped, trained, exercised, and led.

In the NATO Executive Development Program (NEDP) cycle of 2013/2014 the two principal NATO agencies asked young leaders in NATO to explore Multina-

[15] NATO defines information superiority as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

[16] *NATO C4ISR Comprehensive Approach* (Brussels: NATO C3 Board and NC3A, 11 November 2009).

[17] "Establishment of a C4ISR Integration Fund" (Brussels: NC3A, 2010).

[18] The new approach to defense spending during tight economic times—Smartf Defense—was defined by SecGen Mr. Rasmussen as "ensuring greater security, for less money, by working together with more flexibility." As part of this approach, he advocated for nations to "pool and share capabilities, to set the right priorities, and to better coordinate our efforts."

tional Cooperation[19] facilitated by the NCI Agency and NSPA. In the 2015/2016 cycle of NEDP, the Defense Investment division used the same mechanism to assess Smart Defense five years in the future.[20]

As an element of Smart Defense in the NCI Agency, an approach was developed to support nations in re-using NATO common funded solutions for faster, *born-interoperable*, and secure solutions in the area of C4ISR. This initiative was presented at the annual CIO conference in NATO as a program "NATO for Nations" to support the Smart Defense and Connected Forces initiatives of the NATO Secretary General. This program's implementation is based on the "NATO First" solution offered to Nations through the Agency Catalogue.[21]

Again, the Agency decided to benefit from the NEDP class of 2015/2016 and initiated a study on the implementation of the "NATO First" solution[22] in support of Smart Defense and Connected Forces initiatives. Initially, the main driver for the development of the "NATO First" solution for NATO Force Structure (NFS)[23] was the Afghanistan Mission Network (AMN) initiative in response to the request by General McChrystal to have one Command and Control (C2) network for ISAF in 2009.[24]

The decisions made at the Wales Summit to establish the Readiness Action Plan (RAP) and to support it with NATO Force Integration Units (NFIU) in eight Eastern European NATO Nations changed the situation dramatically with the development of the NATO force structure, the establishment of multinational formations and a definition of the model for a forward presence on a rotational basis with an extended exercise program of some kind of "Connected Exercises."

Based on the experience gained with "NATO First" in supporting the NATO Force structure, many NATO partners such as Finland and Sweden started to use NATO tools in their processes for enhanced NATO Response Force (eNRF) and RAP implementation. These efforts included the deployment of eight NFIUs in a very short period in parallel and transforming the C2 system of Multinational Corps North-East in Poland and deploying a new Multinational Division South East HQ in Romania. To address this challenge, the report from the 7th Cycle NEDP project on "NATO 1st, Sharing Alliance Capabilities with Nations" internally

[19] "Smarter Smart Defense: Multinational Cooperation Facilitated," NATO Executive Development Program (NEDP) Project Report (NCI Agency and NSPA, NATO HQ, 2014).

[20] "Smart Defense: Five Years on – Making Smart Defense Even Smarter!" NEDP project report (Brussels: NATO HQ, NCI Agency, 2016).

[21] *Customer Service Catalogue*, *Part I: Customer Handbook* (NCI Agency, 2015).

[22] "NATO First: Sharing Alliance Capabilities with Nations," NEDP project report (NCI Agency, 2016).

[23] "NATO 1st Solution *for NATO Force Structure*" (NCI Agency), accessed October 29, 2018, https://www.ncia.nato.int/Documents/Agency publications/Brochure NATO 1st Solution for NATO Force structure_WEB.pdf.

[24] McChrystal, *My Share of the Task*.

for NCIA, a program to support these various projects with different funding models, but similar requirements were established.[25]

With the decisions at the Warsaw Summit for the *Forward Presence* in Eastern Europe and its enhanced and tailored models, the need for more formal program management was evident to the leadership of the NCIA and so a partnership model[26] for this endeavor was explored.

NATO/EU Readiness and Interoperability in Eastern Europe – C4ISR Perspective

NATO agreed on a Readiness Initiative in 2018,[27] under the notion of *The Four Thirties*, that by 2020 the Allies would be able to have 30 mechanized battalions, 30 air squadrons, and 30 combat vessels ready within 30 days or less. This big change began in Wales in 2014 with the initiation of the Readiness Action Plan, followed by the Warsaw NATO agreement on Forward Presence in parallel with closer coordination with the EU on areas such as mobility, cyber defense, hybrid warfare response, and resilience at large. NATO has always been an alliance of interoperability between members but, with the Interoperability initiative at Wales Summit (2014), it has become a platform to boost interoperability with key partners as well, based on the experience of ISAF and other operations.

In this context, and based on experience going back to 2002 (more than 15 years of development) a framework is proposed for the *(Communications & Information) Program "Readiness and Interoperability (Cyber Resilience)" (PRI)* with an initial focus on the Bucharest 9 countries (Bulgaria, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia). These are nations that have moved from the Warsaw Pact to NATO and the EU in the last 20 years and form a potential framework of nations for rotational battle groups and other formations in the scope of *Forward Presence* as well as other related initiatives. These would include US troops under the *Atlantic Resolve/European Defense Initiative*, but would also include the further development of multinational formations in Eastern Europe, including the evolution of KFOR and Althea as key elements of multinational military presence in Southeast Europe.

Such a program would begin with the identification of the force structure in Eastern Europe. These might include different NFS elements, other multinational formations under NATO or EU initiatives (for example, in Southeast Europe, the HELBROC Battle Group comprising Greece, Romania, Bulgaria, Cyprus and with participation from Ukraine and even SEEBRIG, established in 1999 as an instrument for regional defense cooperation in SEE) and elements of the national force

[25] "Initiative for NATO Forces Readiness and Interoperability Partnership (NRIP)," Enclosure 2 to NCIA/DM/2016/02367 (NCI Agency, 2016).

[26] "NATO 1st Solution (N1S) Concept: Partnership with Customers," Enclosure 3 to NCIA/DM/2016/02367, NCI Agency, 2016.

[27] The SecGen, Mr. Stoltenberg, said in June 2018: "This Is not about setting up or deploying new forces, it is about boosting the readiness of existing forces."

structures of the host countries to be included in such large scale interoperability and readiness endeavor.

Stakeholders in PRI would be the nations whose force structure elements are covered and leadership of the multinational formations addressed plus the strategic commands, respective NATO committees, boards, and related elements on the European defense side. Moreover, the *B9* (Bucharest cooperation) format can be seen as an excellent platform for transforming NATO-EU cooperation by introducing a new approach to modernizing the forces of the nine Nations, increasing their NATO/EU readiness and interoperability (including cyber resilience), and integrating them with the forward deployed forces of other NATO/EU nations on a rotational basis, as well as participation in any expeditionary or intervention forces of NATO or the EU.

Poland, Romania, and Bulgaria could, potentially, benefit most from effective and efficient rearmament and a new level of readiness and interoperability of the force structures in CEE. This would also be for both NATO and EU purposes, but, first of all, for deterrence and defense to the East and, possibly, the South-East through a real federation with NATO/EU systems. B9 is providing a solid basis for the development of PRI as a practical aspect of cooperation in both the NATO and EU context with the close support of NATO Communications and Information Agency for the C4ISR capabilities development and service provision.

There has been an effort on the Bulgarian side since 2014 to define a National Program called "Bulgaria in NATO and the European Defense" with focus on rearmament. It is now moving towards some real projects which have been approved by the Parliament. The most recent—Vision 2030—has civilian support and is a comprehensive and strategic approach to rearmament and close cooperation with B9 Allies. From a Bulgarian perspective, including Albania, Montenegro, and North Macedonia is of critical importance and, in cooperation with Greece, this will change the defense posture in the region. The next step will be to engage with Bosnia and Herzegovina, Kosovo, and Serbia.

Being both NATO and EU members, the Nations of B9 are in a position to harmonize their requirements and to use all available NATO, EU, and multinational/ regional instruments to build the best possible C4ISR/Cyber capabilities for their armed forces in the context of multinational NATO/EU force structures. In addition to B9, the involvement of Adriatic countries such as Albania, Croatia, Montenegro, Slovenia, and North Macedonia (soon to be a 30th member of NATO) plus some Black Sea candidates for NATO/EU membership, such as Ukraine and Georgia (and even Moldova) could be considered under the partnership arrangements.

In this context, a program of "Readiness and Interoperability" for *B9+* nations with the participation of leading battle groups and/or rotating forces from other NATO nations in the region is a logical construct. The program could be supported by NCIA in the context of a "NATO First Solution" with customer funding (including available *common funding* from existing and future *C4 Trust Funds*). In the past, and certainly in the future, the main effort under the PRI will include a

lot of case by case, but urgent and operations-related activities and exercise requests, anticipating rapid reaction.

NCIA did a study on external (non-common funded) customer-support with the *Network Centric Operations Industrial Consortium (NCIOC)* to define the most adequate model, based on the best practices from industry for meeting this challenge. This is a good basis for providing support to outside customers under PRI without interfering with the common funded programs.

Obviously, the C4ISR/Cyber domain is driving innovation, not only in the technology area but in all other aspects, including business models for cooperation and developing required institutions to make this effort a success for all. In this context, the discussions on NATO Allied Command Transformation (NCIOC-ACT) about the adoption of interoperability verification before the acquisition of goods and services are providing additional incentives for PRI. The *Interoperability Verification Initiative* could start ground-breaking projects to develop a new standard in procurement practice that examines enterprise-level interoperability for the Federated Mission Networking environment. This is expected to save billions of Euros for NATO, its members, and partners with obvious benefits for B9+ Nations.

So, there is now an opportunity to review C4ISR/Cyber related projects and programs in the B9+ countries in the context of implementing RAP/FP and Readiness Initiative/ Interoperability Initiative and to consolidate the work in the NATO/EU context for saving money. Perhaps more important will be the ability to achieve a high level of interoperability, security, and readiness of the C2 system on the Eastern Flank with the inclusion of regional countries with troop rotations involving members and partner nations. NATO HQ, the strategic commands, NCIA could play a role, but ownership is for the B9 countries with the involvement of industry and research institutions for the transformational PRI. There will also be a benefit for European defense developments with PRI.

Since its establishment in 2012, the NCI Agency has, by merging the various five NATO C&I agencies, had a declared initiative for the National Chief Information Officers (CIO), together with ACO, ACT and NATO HQ representatives of NFS, research institutions, and industry to define the most effective, efficient and cyber-resilient way to interoperability and readiness in the area of C&I. Their, now traditional, annual CIO conferences[28] paved the way to implementing the NATO First Solution and achieving interoperability and readiness in a secure environment by fast, easy, and affordable ways (NATO R&I SAFE).

Defining PRI as the result of the NATO/EU led review of requirements with the active implementation of FMN compliant solutions in cooperation with industry and the NCIA as an executive/support agency will bring practical aspects of Interoperability and readiness to a new level in Central and Eastern Europe. PRI needs to be fully synchronized with all exercises involving forces in CEE with

[28] For information on each in the series of "Chief Information Officers" conferences see the website of the *NCI Agency*, https://www.ncia.nato.int.

NATO/EU operations, missions, activities, and tasks for not just continuous improvement of interoperability and readiness, but also to enable them to provide a real contribution to deterrence and defense. In parallel, consideration should be given to extending PRI to all "new" NATO Nations in CEE as well as to define PRI Partners to support work with the partners in CEE (including Western Balkans and Black Sea region).

Conceptualization of the scope and Governance/Management of PRI could be done in the larger environment of Industry and NGO consultations, but real steps could be taken only by Nations or ACO/ACT related EU structures. Of course, existing models, implemented for the AMN/FMN environment as the Distributed Network of Battlelabs (DNBL) as an instrument to support the program, will also be used to shape the program.

Education and Training as Major Tools for Interoperability. Implications for the Western Balkans and the Black Sea Region

When it comes to readiness and interoperability, especially of multinational formations, it is not just about the equipment but also about people and their education and training. This is the reason to consider the network of multinational formations in CEE as instruments to foster cooperation in the area of education and training, certification, and development of personnel. It is evident that for multinational formations, including on the tactical level (battalion battle groups, air squadrons, ships deignated for the Readiness initiative, for example), the operational language will be English, the procedures will be NATO-based, and C2 will require NATO First Solutions.

For these reasons, the synchronization of education and training programs for officers, non-commissioned officers, and even soldiers has to be achieved around NATO standards. Equally important is the experience from rotation in multinational units. The Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, together with the NATO Defense Education Enhancement Program, is already providing a lot through their joint work on reference curricula in various fields.[29] These curricula bring the Professional Military Education of NATO allies and their partners closer together, enhancing standardization and also improving intellectual interoperability. The same is true for the efforts of the European Security and Defense College, which is part of the European External Action Service. It has focused efforts to bring common standards to education and training in EU-wide professional military education.[30]

[29] See "Generic Officer Professional Military Education – Reference Curriculum," "Cybersecurity – A Generic Reference Curriculum," and "Non-Commissioned Officer Professional Military Education – Reference Curriculum," all avialble on the NATO website, https://www.nato.int.

[30] European Security and Defense College (ESDC), "Standard Curricula," accessed October 29, 2018, https://eeas.europa.eu/topics/common-security-and-defense-policy-csdp/4369.

While it is often important to distinguish between education and training, in this article the view is taken that they are mutually inclusive activities. Education and training, together with experience, are necessary for the complete development of military personnel. Interoperability in both education and training is the critical gateway to endow a nation's armed forces with the ability to live up to and to meet national security responsibilities in an international security environment where working closely with Allies and partners is crucial. Thus, the proposal to concentrate further efforts of NATO and the EU in the Western Balkans and the Black Sea region in order to meet the current security challenges via academic dialogue and interoperability in professional military education and training. This will provide a steady basis for delivering on Deterrence and Defense and for projecting stability in the regions.

Conclusion: Regional Cooperation (SEDM/A5 and B9): Is Consolidation Possible?

An analysis of the development of the NATO/EU presence in Central and Eastern Europe, especially through multinational formations—from KFOR to battle groups of eFP in Baltic states and Poland, the EU battle groups (as HELBROC in South-Eastern Europe) on the first level, followed by division/corps level HQs and up to NCS—provides an input to identify the requirements for interoperable C2 systems at a tactical level, directly connected to operational/ strategic level and respective training requirements for the personnel in these multinational formations.

Even more serious is the challenge to define the roadmap for the development of these multinational formations in Eastern Europe in a NATO/EU framework with the participation of the Western European and North American members of the Atlantic Alliance. It is important to stress that multi-nationality on a tactical level—in battalions, squadrons, and ships—is what matters most of all. This is because it is about the real use of NATO procedures on a daily basis, C2 systems, and the demonstration of solidarity. These tactical units, being multinational, will be a model for the national units of the same type or size but, being under multinational governance, C2 will maintain the readiness and interoperability required by the Readiness Initiative, and so they will have better chances to be committed for deployment without caveats.

Based on the large pool of multinational tactical units, it is much easier to nominate higher level multinational HQs for the management of training and readiness and for planning and C2 in case of activation. Such organizations will facilitate multinational projects for C4ISR interoperable systems and other equipment and/or armaments as well. These multinational projects could be managed by extended national agencies but maybe an even better option is to use NCIA/NSPA.

The last but not least is the organization for the education and training, covering all facets from individual to collective and from field to computer assistance.

The main message in this article is that if NATO is to mature by consolidating the existing structures of multinational formations and develop a roadmap for its further development in CEE/SEE with a special focus on multinational C4ISR projects and joint education and training focused on interoperability and readiness, the landscape of security and defense could be changed dramatically. Real transformation in defense could take place in the region and, as a result, overall resilience will be improved.

Further research is required to develop the business case for a Program for Readiness and Interoperability, to define the governance and management model for the program, the technology roadmaps and specific requirements for education and training (including exercises), and for the implementation of a forward presence in CEE/SEE that will foster NATO-EU and regional cooperation.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Authors

After 19 years in the military, Dr. Velziar **Shalamanov** followed by an academic career in the Academy of Sciences mixed with several tours of public service: Deputy Minister of Defense (1998-2001), Minister of Defense (2014) and Director Demand Management in the NATO's IT and Cyber Agency (2009-2017). Currently, he is focusing on the consolidation of the academic cyber capacity in Bulgaria. In parallel, he is engaged in politics and NGOs pursuing better positioning of Bulgaria in NATO and European defense, the information society and improvement of research governance. *E-mail*: shalamanov@acad.bg.

Mr. Pavel **Anastasov** has been heading the Unit for Strategic Policies and Analysis in the Cabinet of the President of the Republic of Bulgaria in the period 2012-2014. He served as deputy minister of defense in 2014. In the period 2014-2018 he has been working on Black Sea Security issues in the Political Affairs and Security Policy division at NATO HQ.

Dr. Georgi **Tsvetkov** is assistant professor at the "G.S. Rakovski" National Defense College in Sofia, covering various topics in the area of defense management, capability development and security policy.

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Rosław Jeżewski, *Connections QJ* 18, no. 1-2 (2019): 43-60
https://doi.org/10.11610/Connections.18.1-2.03

Research Article

Cross-domain Coercion as Russia's Endeavor to Weaken the Eastern Flank of NATO: A Latvian Case Study

Rosław Jeżewski

Abstract: Cross-domain coercion is tangible on NATO's Eastern flank and characterized by the use of derogatory propaganda, fake news, financial assets in the Latvian banking system, Russian-based organized crime, and various military elements. This study on cross-domain coercion, however, concentrates on the cohesion of the Latvian population, existing gaps within society, and its susceptibility to being exploited by Russia. To acquire data for this study, the author conducted interviews with representatives of the Eastern flank countries and performed an extensive literature review. To determine the root causes of vertical division in the society, the "5 WHYs" method was used. This study proved that the presence of a Russian minority and the Russian-based organized crime minority can be a good base to create unrest and that Russia is able to influence the internal policy of a country when the Russian economic footprint exceeds 12 % of GDP. The demographics and the cohesion (including vertical and horizontal divisions) of the society are factors determining the resistance of Latvia. The triumph of the populist parties during the October 2018 parliamentary elections reflect the trend that the nation is tired of the corrupt and ineffective government rather than that it is drifting towards Russia. In a broader scope, it is expected that cross-domain coercion will increase and Russia will test the cohesion of NATO.

Keywords: NATO, Eastern Flank, Latvia, cross-domain coercion, Russia, organized crime, economic footprint, Latvian resistance, corruption.

Introduction

Vladimir Putin said that he wished the Soviet Union had not collapsed; for him and many Russians, this had been a geopolitical hecatomb, which removed East-

Creative Commons BY-NC-SA 4.0

ern Europe from Russian hegemony.[1] The fact that the Baltic countries and the majority of the former Soviet zone of influence are now part of NATO makes Russia furious. The Kremlin has been bombarding them with fake news, and with accusations of fascism and Nazism, hoping to find a weak point in the structure of the Alliance. The Eastern flank of NATO is not homogenous, especially when it comes to the Baltic States. The question is which of the three Baltic countries is the most vulnerable?

A brief quantitative analysis of a few indexes helps to find an answer. The European Quality of Government Index for 2017 ranks Estonia in the 90th position (score: 54.4 points), Lithuania in 114th position (score: 43.6 points), and Latvia in 142nd position with the score of 38.2 points. Another indicator can be the Human Development Index, where, again, Estonia has the best position among the Baltic states (30th position with the result of 0.871), then Lithuania (35th position with the result of 0.858), and again Latvia was the last country, ranked as 41st with the result of 0.847. The same sequence was observed in two other indexes: the Social Justice Index for 2016 (Estonia: 6.15, Lithuania: 5.69 and Latvia: 5.04) and the Social Cohesion Index (Estonia: 5.85, then Lithuania: 5.69, and finally Latvia: 5.10). There are also qualitative indicators that help in giving Latvia the lowest rank, such as 26% of the Latvian population are ethnic Russians, there are numerous non-citizens, the society is troubled and is still recovering from the 2008 financial crisis. This makes Latvia especially vulnerable to New Generation Warfare and cross-domain coercion, which has been a challenge to the security of the Baltic States.

Russia is very unhappy about Latvia's membership of NATO and will attempt, by any means below the threshold of war, to both undermine the country's stability and to affect the cohesion of its population, hoping also to weaken the unity of NATO. The National Security Concept[2] of the Latvian Ministry of Defense states that in this pursuit Russia will coerce all accessible domains, especially social, economic, and military.

There are several examples of Russian coercion in Latvia[3]: derogatory active propaganda from Russian sponsored mass media, Russia's live-fire drill within the Latvian Exclusive Economic Zone in April this year and the activities of Russian-based organized crime. These are difficult to counter by conventional

---

1 Adam Taylor, "Putin Says He Wishes the Soviet Union Had Not Collapsed. Many Russians Agree," *The Washington Post*, March 3, 2018, www.washingtonpost.com/news/worldviews/wp/2018/03/03/putin-says-he-wishes-he-could-change-the-collapse-of-the-soviet-union-many-russians-agree.

2 "The National Security Concept (Informative section)" was released to public in 2014. The details about possible Russian Course of Action can be found on pages: 4 (hybrid activities), 15 (threats to the unity of the society) and 18 (propaganda), https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.

3 Also in Estonia. For details see: Rachel Marie Casselman, "Russia's Hybrid Warfare: The Prowess and Limitations of Putin's (in)Visible Hand in Estonia and Latvia," Master of Arts Thesis (University of Oregon, June 2017), https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/22759/Casselman_oregon_0171N_11972.pdf.

means, as the Russian idea of waging low-level conflict gives it an advantage over the formalized response system, especially when it comes to Article 5 scenarios for NATO countries.[4]

The employment of New Generation Warfare against Latvia is unlikely to lead to any form of conventional war. Russia has been employing the tactics of raiding, which is especially lucrative and efficient in a confrontation with a stronger opponent.[5] It is a cheap and efficient form of warfare; it crosses many domains (cyber, informational, financial), includes infiltration and surprise attack, leverages agility, and helps to achieve the desired political result.[6] The literature study[7] made for this article leads to the conclusion that it can be successful in targeting the various vulnerabilities that exist or will be existing within Latvian society, undermining the government's credibility, and thus weakening the cohesion of the society.

Firstly, Latvia has the biggest population of ethnic Russians in Europe (nearly 26%). Many of these people are non-citizens who are deprived of voting rights and cannot possess any land or property. This makes them the target for Russian psychological operations, with Russian propaganda in the lead, trying to convince the Russian ex-patriots that Latvia is such a bad ally of the West and does not protect their rights. Secondly, there is evidence of Russian-based organized crime operating in Latvian society. Criminal gangs are suspected of money laundering and close cooperation with the Kremlin during covert operations against Latvia's society and government (for example, participation in intelligence operations). The scope and size of this factor have not been publicly disclosed, but the available data indicates that, despite being barely visible, it has had a profound effect on the Latvian security system. Thirdly, the country has a grave social problem, which is an amalgam of income inequality, an aging population (due to low fertility rates), and emigration.

This qualitative study will explore questions like: Is the presence of the Russian minority in Latvia a threat to the country's cohesion? What is the impact of Russian-based organized crime on Latvia's stability? What is the nature of Russian hostile activities against Latvia? What possible countermeasures can be

---

4 Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," *Proliferation Papers* 54 (French Institute of International Relations, November 2015), 39, https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

5 Michael Kofman, "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," *War on the Rocks*, June 14, 2018, https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition.

6 Kofman, "Raiding and International Brigandry."

7 The vulnerabilities theme as Russia's target is reflected in works of: Janis Berzins, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," *Policy Paper* no. 2 (Riga: National Defence Academy of Latvia, April 2014), 12, https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf; "The National Security Concept;" James K. Wither, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87.

used against these factors? To find the answers to these questions, it is necessary to start with a survey of the Latvian people, without which it would be difficult to determine what gaps and vulnerabilities may exist in the population and how cohesive that population is. The next step will be an assessment of the susceptibility of the Latvian population to exploitation by Russian propaganda and the attitude of the Russian minority, including the threat perception of Latvians and ethnic Russians. The author's intent is also to find out how deeply Russian-based organized crime (RBOC) has penetrated the Russian minority and what the relations between RBOC and other malign actors are.

Finally, the author will speculate if and when Russia can violate Latvian living space by employing cross-domain coercion and will summarize the course of the research. The data for this study will be sought from interviews with Latvian (PASS 18-16, SHAPE NMR personnel, think-tank members) and Polish (think-tank member) personnel, supported by an extensive literature search. The approach to solving this problem will be Root Causes Analysis (RCA) for a chosen factor to determine its impact on Latvia's living space.

Survey of Latvian Population

The Latvian population is one of the smallest in Europe. Currently, it is estimated at approximately 1,950,000, of which slightly more than one million are economically active.[8] Of the ethnic groups within the country, 62% are Latvian and the largest minority within Latvia is Russian (25.4%), most of whom live in the Latgale district in the eastern part of the country. Many sources mention that Latvia has had long-term problems related to the presence of the Russian diaspora, which is the result of the previous Soviet occupation. It is necessary to note that native Latvians perceive there to be two major groups in the country – Latvian speakers and non-Latvian speakers. It is in the second group where Russian speakers can be found (including ethnic Russians, Belarussians, and others).[9]

Inside the Russian minority, there are non-citizens (approximately 242,000) who have a relatively low status in society due to their inability to obtain good jobs, their poor command of the Latvian language, and the troubled economy in the Latgale district. Most of the jobs available to them are in the transportation sector or on construction sites. Latvia has been suffering from a serious demographic decline; the forecast for 2060 projects a population of about 1,200,000 compared to 1,950,000 at current. Furthermore, it is forecast that by 2030, half of Latvians will have turned 50. Another driver of the decline, as well as aging, is emigration. Many migrants are under 30 years of age,[10] and it is estimated that

[8] *Latvia: Executive Summary* (Englewood, CO: IHS Markit, 2018), 40.

[9] Interview with a Latvian service member, October 8, 2018.

[10] BMI reports that the number of emigrants planning to return to Latvia in the short-run drops from 10% to just 3%. In longer perspective, Latvia's demographic problems will hit the economy hard. More in *Latvia Country Risk Report – Q3 2018* (London, United Kingdom: Business Monitor International, 2018).

the intensive emigration will continue until at least 2030.[11]

This is a grave demographic problem[12] and has a very negative effect on the security system. If these factors are put together with the small population density (4 people/sq. km) it is very likely that some areas of the country will end up being depopulated – which will provide unrestricted conditions in which possible adversary elements could operate, should they appear. The webpage *www.globalfirepowerindex* identifies this as a paramount problem for defense – "Going beyond military equipment totals and perceived fighting strength is the actual manpower that makes up a given military force. Wars, particularly those with high attrition, traditionally favor those with more manpower."[13] In the case of Latvia, the uniformed formations reflect the internal pattern of ethnic diversity: the Latvian National Guard is mostly Latvian speaking, the Army is generally Russian speaking, the Police – half Latvian, half Russian, and the Border Guard in Latgale is mostly Russian speaking.[14]

These findings concerning the cohesion of Latvia's population differ, especially when comparing the literature study with the private interviews. The picture of the population presented during one private interview in September was that the nation is strong and cohesive and that this does not concur with the derogatory messages from its big neighbor.[15] Another Latvian official[16] stated that the nation is rather cohesive and tired of the government scandals and corruption; cohesion is present in the rural areas where Latvians and Russians coexist in compact communities, but society is polarized in the big cities, especially in Riga and Davgapilis.

However, there is a report in which society is described as being divided, and that people in Latvian society are neither socially nor politically active,[17] and that the population seriously distrusts the government.[18] The same document claims that the participation of society in public issues is low.[19] Another brief summary about Latvian cohesion comes from the EU Social Justice Index, 2017, in which it is said that Latvia has reached 19th position among the 28 other EU members (the last among the Baltic States) with a score of 5.46 on the Social Justice In-

---

11 *Latvia Country Risk Report,* 20.

12 *Latvia: Executive Summary*, 40.

13 "Latvia Military Strength," *GlobalFirepower.com*, https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=latvia.

14 Interview with a Latvian government official, October 8, 2018.

15 Interview with a Latvian servicemember, September 12, 2018.

16 Interview with a Latvian government official, October 8, 2018.

17 Ieva Bērziņa, Janis Berzins, Martins Hirss, Toms Rostoks, and Nora Vanaga, *The Possibility of Societal Destabilization in Latvia: Potential National Security Threats* (Riga: National Defence Academy, Center for Security and Strategic Research, 2018), 14, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/WP%2004-2016-eng.ashx.

18 Bērziņa, *et al.*, *The Possibility of Societal Destabilization in Latvia*, 5.

19 Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 14.

dex.[20] The education system was especially well evaluated, but it was remarked that there is an urban-rural gap, while education chances for those with special needs are limited."[21]

Despite positive trends, the economy has significant vulnerabilities, which include being a small and open system dependent on global trends. Business and development is usually associated with Riga, while the rest of the country is underdeveloped. This is the reason why about 30% of native Latvians have declared their readiness to leave the country. There is a significant disparity in the rate of unemployment, with the best situation in Riga and the worst in the Latgale region. The structure of the governmental organizations is outdated and does not provide proper services for the rapidly declining population. Pensions are so low that people are being driven into poverty. As a result, the percentage of the older generation facing the risk of social exclusion has risen from 33% in 2011 to 43.1% in 2018.[22] These factors affect the cohesion of the Latvian community. But it also has an extra internal problem – the attitude of the Russian minority.

Attitude of Russian Minority towards Latvia

First impressions from the literature study lead to the conclusion that the threat from the Russian minority is low[23] since about 80% of Russian speakers declare their loyalty to the nation.[24] The diaspora is reasonably integrated within society, although there is some resentment towards any active participation in the defense system.[25] There is also the general opinion that the forthcoming language reform will bring many problems, and that may result in feelings of discrimination.[26] Probably this is the reason why these people are not willing to engage in public protests. Half of these non-citizens do not support Russian accounts,[27] and the older generation expresses the greatest level of loyalty[28] to Latvia; they profess to enjoying life in Latvia and prefer it to Russia. However, a majority of them claim that they do not plan to obtain Latvian citizenship, and the reasons are:

---

[20] Daniel Schraad-Tischler, Christof Schiller, Sascha Matthias Heller, and Nina Siemer, *Social Justice in the EU – Index Report 2017* (Gütersloh: Bertelsmann Stiftung, 2017), 49, https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/Graue Publikationen/NW_EU_Social_Justice_Index_2017.pdf.

[21] Schraad-Tischler, et al., *Social Justice in the EU*, 115.

[22] Schraad-Tischler, et al., *Social Justice in the EU*, 12.

[23] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 13.

[24] Aleksandra Kuczyńska-Zonik, "Non-Citizens in Latvia: Is it a Real Problem?" *Sprawy Narodowościowe Seria nowa* (*Nationalities Affairs New series*) 49 (2017), Article 1438, https://doi.org/10.11649/sn.1438.

[25] James K. Wither, "'Modern Guerrillas' and the Defense of the Baltic States," *Small Wars Journal*, January 13, 2018, http://smallwarsjournal.com/jrnl/art/modern-guerrillas-and-defense-baltic-states.

[26] *Latvia: Executive Summary*, 21.

[27] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 10.

[28] Kuczyńska-Zonik, "Non-Citizens in Latvia: Is it a Real Problem?" 8.

the problems with communicating in the Latvian language, ease of traveling to Russia (no visas are necessary) and, partially, plans to obtain Russian citizenship.

The other interviews with Latvian representatives produced more details. One of them expressed some rather negative feelings towards the non-citizens claiming that their existence is a real problem for his country. According to his statement, these people love Russia but live in Latvia; some of them have problems with alcohol and drugs, especially the younger generation (of non-citizens); the older generation accuses the Latvian population of Nazism. But there were also positive points during this conversation – it was said that much depends on the parents of the younger non-citizens. There are some who try to learn the Latvian language and to integrate within the society. Another Latvian representative[29] stated that those non-citizens who wanted to emigrate to Russia had already emigrated, and now the majority of them do not plan to emigrate. The older people feel some sentiment towards Russia, but only because of their ethnicity. They definitely do not want to emigrate, especially to Russia, as they get information from the younger generation about real living conditions in Russia and Latvia. They are partially influenced by Russian propaganda, especially in the Eastern part of the country and, having a free visa, like to travel to Russia.

But there are also non-citizens who act against Latvia, and that creates problems for national security, given that they can be used by the Kremlin as a tool. A first warning signal comes from the NATO Centre of Excellence, which reveals that Russia is seen as a trusted source of information for minorities in the Baltic States.[30] Versions of a document developed by Latvia Security Police paints a clearer picture. This 2017 Report[31] claims that there are Russian compatriots who were involved in Russia's misinformation campaign, in which Latvia was targeted, and its internal problems were exaggerated.[32] Probably this section of the Russian minority may be used again if Russia wants to influence Latvia's internal situation.[33] So far, there have been several cases in which some activists were so advanced in their derogatory activity fomenting hatred and intolerance, that Latvian Security Police have had to intervene and warn them about the consequences of any further behavior of this kind.[34] One of the tools of incitement may be Russian-based organized crime (RBOC), which has penetrated the Russian diaspora. It is directly connected to the Kremlin, from where it receives sup-

[29] Interview with a Latvian government official, October 8, 2018.

[30] Ieva Bērziņa, Māris Cepurītis, Diana Kaljula, and Ivo Jurvee, *Russia's Footprint in the Nordic–Baltic Information Environment*, Report 2016/2017 (Riga: NATO Strategic Communications Centre of Excellence, 2018), 102, www.stratcomcoe.org/russias-footprint-nordic-baltic-information-environment-0.

[31] *Public Report on the Activities of Latvian Security Police in 2017* (Riga: Latvian State Security Service, 2018), 19, URL: https://vdd.gov.lv/en/useful/annual-reports.

[32] "Public report on the activities of Latvian Security Police," 19.

[33] "Public report on the activities of Latvian Security Police," 20.

[34] "Public report on the activities of Latvian Security Police," 15.

port and directions as to how to wield political influence and to be an instrument of statecraft abroad.[35]

Further research concerning the perception of threats to Latvia's security has brought surprising findings. For Latgalians, Russia is one of their least problems, which is thought-provoking given the location of the district. 78% of people who speak the Latgalian dialect claim to support Latvia when faced with Russian aggression. They claim to be ready to fight for the freedom of Latvia if that is necessary.[36] But, for the Latvian population, the biggest threat is not Russia, but the troubled domestic situation (low wages, the bad demographic situation, an inefficient health care system, corruption, and crime).

As for the interviewees, all of them considered Russia to be a threat.[37] They also expressed the feeling that Russia could attack their country without any warning. This is confirmed by entries in the Latvian "National Security Concept," where Russia is recognized as the main threat to Latvia's national security. Other statements in the document point out that Russia implements its foreign policy by using complex measures, so-called hybrid threats, which aim to gradually weaken the countries at which they are aimed.

Based on these insights, it is possible to speculate that the Russian diaspora in Latvia is not homogenous, it differs in opinion towards the government and it has different perspectives about the threat from Russia. That is why this subject definitely requires further studies and interviews, as the current postures of the non-citizens and their Russian compatriots are not well reflected in the literature. This also refers to the presence of Russian-based organized crime, which has penetrated the Russian minority in Latvia.

The Impact of Russian-based Organized Crime on Latvia

The origin of Russian-based organized crime (RBOC) structures in Latvia stretches back to the Soviet times, when many criminals, who were released from prisons, decided to go to Latvia and start a new life there.[38] In this context, the term "new" means criminal, as these people kept their underworld inclinations and connections in order to use them in their new homeland. As cooperation grew, so did crime in Latvia in areas of drug trafficking, car theft, money laundering, and fuel smuggling. For example, in 2012, it was calculated that 30% of fuel consumption in Latvia came from contraband supplies.

---

[35] Riga is considered one of the criminal hubs specialized in money laundering. See Mark Galeotti, "Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe," European Council on Foreign Relations, April 18, 2017), www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

[36] Interview with a Latvian government official, October 8, 2018.

[37] Following these statements, Russia and Belarus should be perceived together as threat, where Belarus can be the proxy.

[38] Walter Kegö, et al., *Russian Organized Crime: Recent Trends in the Baltic Sea Region* (Washington, D.C.: Institute for Security and Development Policy, 2012), 69, http://isdp.eu/publication/russian-organized-crime-recent-trends-baltic-sea-region.

John Ruehl argues that Russia, despite being weaker, is still able to coerce many countries, including the USA. The Russian toolkit includes the use of minorities, cyber and info operations, natural resources, and the RBOC. This development was possible because, as the author points out, there was an agreement between the Kremlin and RBOC about mutual support, which resulted in the building of mafia-like structures and networks of corruption in Europe, enabling Russia to create zones of influence.[39] This makes the RBOC a proxy agent of Russian interests, which can promote the Russian agenda wherever it is feasible.[40] A further study of RBOC activity in Latvia has revealed that when the Russian economic footprint in a country exceeds 12% of GDP, it creates conditions that allow for the RBOC to use the economic channels.[41] Since there is close economic cooperation between Latvia and Russia, many links have been created between Latvian and Russian businesspersons with Russian-backed crime elements in the background.[42]

RBOC also has a second face, which is connected to and directed by the Russian special services. It has been used by the Kremlin as a channel for intelligence and political influence,[43] and it is becoming a real problem while Russian attempts to undermine Western cohesion continue. Russian criminal groups, which are located on Latvian territory, are employed by the Russian security services to gather information about the border area (Latgale), security installations, and the personal data of prominent persons.[44]

Information about Russian-based organized crime (RBOC) in Latvia is limited. However, a few aspects need to be considered here. A short outline of its activity in Latvia leads to the conclusion that RBOC has penetrated the Russian diaspora and has good knowledge of local criminal structures. There is close cooperation between elements of RBOC and Russian special services, including cybercrime. And, RBOC follows the economic involvement of Russia. It means that this low-profile element has a significant potential to operate inside Latvia, probably following instructions from the Kremlin. In the face of low social activity in Latvian society, this creates permissive conditions for the easy weaponization of Latvian

[39] John Ruehl, "How Is Russia so Dangerous with an Economy Smaller than Italy's?" *PoliticsMeansPolitics.com*, April 21, 2018, 6, https://vip.politicsmeanspolitics.com/2018/04/21/how-is-russia-so-dangerous-with-an-economy-smaller-than-italys.

[40] Ruehl, "How Is Russia so Dangerous with an Economy," 6.

[41] Heather A. Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov*, The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Center for Strategic and International Studies, October 13, 2016), 18, https://www.csis.org/analysis/kremlin-playbook.

[42] Conley, et al., *The Kremlin Playbook*, 48.

[43] Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services* (European Council on Foreign Relations, 2016), 4, https://ecfr.eu/publication/putins_hydra_inside_russias_intelligence_services/.

[44] "Public Report on the Activities of Latvian Security Police," 9.

society, for example, by the employment of Latvian criminal groups (cooperating with RBOC).

How Russia "Weaponizes" Latvian Society

The weaponization of identity, which is understood here as inciting the Russian minority against the Latvian government and the state, has been reflected in many publications. At this point, it is a good idea to start with the statement in "The National Security Concept"[45] (likely regarding Russia), which talks about "attempts of separate countries to influence the unity of Latvian society." In addition, Janis Berzins argues that Russia can employ the language reform to create discord between the Latvian population and national institutions.[46]

In the course of weaponization, Russia is using the strategy of raiding, which is a cheap means of warfare.[47] When there is a situation in which the traditional (conventional) methods are too expensive, raiding is easy and effective; in the information sphere, it shapes the perspective to reach the desired effect, which is coercion of the enemy.[48] As in every aggression, the intruder targets the center of gravity of the opponent, and, in the Latvian case, it is probably the public perception.

Myriads of derogatory messages penetrating the Latvian information space have been sent to try to create a positive picture of Russia in the eyes of the Russian minority in Latvia and to undermine trust in the Latvian government. Whilst there are broadcasts of music and culture, in between, there is also fake news and lies (like the one that Latvia was never occupied by Russia). Russian media enjoys an easy ride in the Latvian information sphere, which hosts media in both Russian and Latvian. TV, radio, troll farms, and also robot-trolling transmit Russia's soft power in the social media and also counters the messages of other competitive actors. Russia plays on the national sentiment of the Russian minority in order to influence the domestic policies of neighboring countries, even using these people as a means of implementing foreign policy. Probably the most accurate description of this comes from the NATO Strategic Communications Centre of Excellence (COE), which states that "the violation of the human rights of Russia's compatriots abroad may be used as justification for the violation of sovereignty, as was the case during the war with Georgia and crisis in Eastern Ukraine."[49] It is possible to speculate that if Russia decided to project instability, the minority would be a tool.

The danger related to this activity is pinpointed by the Constitution Protection Bureau, which in 2016 reported that "Russia's influence in Latvia's infor-

---

[45] *The National Security Concept (informative Section)* (Riga: Ministry of Defense, 2018), 1, https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.

[46] Berzins, "Russia's New Generation Warfare in Ukraine," 12.

[47] Kofman, "Raiding and International Brigandry," 1.

[48] Kofman, "Raiding and International Brigandry," 4.

[49] Bērziņa, et al., *Russia's Footprint in the Nordic-Baltic Information Environment*, 32.

mation environment still constitutes one of the most important long-term threats to the security of the Latvian state." This broadcasting is used to target the many vulnerabilities that exist within society, such as economic diversity, the nation's vertical division, and income disparity. Russia will exploit them all and use any pretext that suits its purpose. In this stream of messaging, Russia presents itself as the defender of old sentiments criticizing NATO and the Latvian language policy and repeating its offers of citizenship and pensions for compatriots. It is aimed especially towards the part of the population that only consumes Russian-language media and, in 2015, a media survey confirmed that "46% of Russian speakers don't obtain any information from the Latvian language media, approximately one fifth of Latvian society cannot be reached through media in the state language."[50]

The easy access to Latvian media space does not guarantee victory for Russia in this information war. A report from the NATO Centre of Excellence survey clearly shows that Russian efforts are not as effective as planned since "national media in the surveyed countries is perceived as a more trustworthy source of information than the Russian media outlets."[51] For example, 54% of respondents to a 2017 public survey fully disagree with the statement: "Russian speaking people in Latvia are being discriminated."[52] In another example, 45% fully disagreed with the statement that "NATO is a threat to Russia."[53] This tends to suggest that the audience makes their judgment of the Russian broadcasting by comparing it with other sources.[54]

The weaponization of Latvian society is not limited only to the information sphere. Russia has been searching for countries or regions with poor governance to gain influence over them by means of corruption.[55] This process is at the forefront of what is known as the New Generation Warfare, which aims to influence a system by penetrating it and weakening from the inside.[56] Once inside, Russia pumps its influence into the country along established economic connections and tries to capture the state and amend national decisions.[57] In May 2018, Reuters placed an article on its website about money, suspected to be Russian, that was kept in the Latvian banking system and was being used to interfere in the internal affairs of European countries.[58] The agency stated that these financial

[50] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 17.

[51] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 90.

[52] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 98.

[53] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 100.

[54] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 100.

[55] Conley, et al., *The Kremlin Playbook*, X.

[56] Conley, et al., *The Kremlin Playbook*, X.

[57] Conley, et al., *The Kremlin Playbook*, X.

[58] These issues are currently under investigation. For more details go to: John O'Donnell and Gederts Gelzis, "Exclusive: Latvia Probes Whether Russian Money Flows Used to Meddle in Europe," *Reuters*, May 29, 2018, https://fr.reuters.com/article/us-latvia-banks-politics-exclusive-idUSKCN1IU2BM.

assets were delivered from Russia and used to finance hybrid activities and to undermine political systems in other countries. One more indicator of these Russian attempts was given in July 2018 by Bloomberg,[59] which reported about suspected financial transactions from Russia between 2010 and 2014, and also a significant inflow of Russian deposits into Latvia beginning in 2012. These deposits are suspected to have been used for organized crime and corruption.

An example from Finland shows a path of financial coercion that leads to an alarming conclusion. In September 2018, there was a massive operation in south-western Finland, when the security services discovered the existence of a Russian plot. Ethnic Russians (some with double nationality) were buying or constructing expensive houses in the proximity of vital communication routes and security installations. They were also buying ex-military speed boats and storing huge amounts of cash.[60] According to some sources, there were frequent helicopter flights between Finland and Latvia. Discussions are now taking place in Finland about introducing strong financial countermeasures, which will reduce the possibility of foreigners buying land or property in Finland. Similar measures could also be introduced in Latvia, where it is possible now to gain 5-year permanent residence by fulfilling one of the three conditions: buying a property, investing, or opening a bank account.[61]

It is also necessary to pay special attention to Russian indoctrination of the young, which is taking place outside of Latvia in the form of paramilitary camps.[62] In these places, young brains are said to be infected with fake history, for example, about the Soviet victory during World War II. This Russian investment in the young generation may result in a batch of pro-Russian leaders who may, one day, try to shape the internal policy of Latvia. President Putin's decision announced on July 26, 2018 about limiting support for the compatriots in Latvia, may seem a bit controversial and signal a Russian step backwards. But it may be only a temporary and rational move, perhaps because of its other areas of interest (Ukraine, Syria). Putin can reactivate pro-Russian sentiments at any moment. Attacks on taboo areas such as language, history, and integration can create a horizontal division that internally weakens the country.

In response, Latvia strives to unite the nation into one cohesive society, which will be able to repel any adversarial action. There has been an official call for the

[59] Aaron Eglitis and Alessandro Speciale, "Latvia's Corruption Scandal Is Getting Even Weirder," *Bloomberg*, July 13, 2018 https://www.bloomberg.com/news/articles/2018-07-13/latvia-s-corruption-scandal-is-getting-even-weirder-quicktake.

[60] Antoni Rybczyński, "'Zielone ludziki' na Bałtyku? Spektakularna Akcja Fińskich Służb," *TVP Info*, October 1, 2018, https://www.tvp.info/39269003/swiat/zielone-ludziki-na-baltyku-spektakularna-akcja-finskich-sluzb/.

[61] More details can be found at: "Latvian (EU) Residency Program," *Elma Global*, www.second-citizenship.org/permanent-residence/latvian-eu-residency-program.

[62] "Saeima Bans Latvian Children's Participation in Paramilitary Camps in Russia," *The Baltic Times*, May 4, 2018, https://www.baltictimes.com/saeima_bans_latvian_children_s_participation_in_paramilitary_camps_in_russia/.

"duty of each citizen to defend their country and to resist an aggression in an active or passive manner."[63] Apart from the Latvian uniformed forces, the core of the deterrence system is the presence of NATO units on Latvia territory, which conduct exercises as a show of force and a show of the NATO flag. On a national level, deterrence capabilities are based on the concept that, besides the existence and training system of uniformed formations, there is the potential to "rapidly increase the extent of these forces for the level required for the deterrence or warfare."[64] This could mean, though, that one of the factors determining the resilience of Latvia's defense system is the aging of the population. Latvia will be facing problems here because "the Baltic states face a common demographic challenge as efforts to expand the size and capacity of territorial forces may be thwarted by a shortage of young, skilled recruits, especially, as seems likely, members of the large ethnic Russian minorities in Estonia and Latvia are unwilling to take part."[65]

Root Cause Analysis: The Case of Vertical Division

Among factors affecting the cohesion of the Latvian population and posing a threat to national security, there is vertical division within society and distrust of the government. At first sight, this may be explained by the presence of the Russian minority, corruption, poor economic conditions, or other factors. Since perception is not enough, the author decided it was necessary to find other reasons for this phenomenon, in other words – root causes, and employed one of the simplest yet most effective research methods – 5WHYs.The idea of this method is iteratively asking questions starting with "Why" to get to the core of the problem. The number of questions does not have to be five; depending on the scale and complexity of the problem, it maybe six, seven, even ten. Based on this, the process[66] began with a statement of the problem:

There is vertical division in Latvian society.

---

[63] Ministry of Defence of the Republic of Latvia, "The National Defence Concept," approved by the Cabinet of Ministers on May 24, 2016, 7, www.mod.gov.lv/sites/mod/files/document/Valsts_aizsardzibas_koncepcija_EN.pdf.

[64] Ministry of Defence of the Republic of Latvia, "The National Defence Concept," 9.

[65] James K. Wither, "'Modern Guerrillas' and the Defense of the Baltic States," 7.

[66] Based on: Una Bergmane, "The Three Little Oligarchs: Latvia's Corruption Scandal," *Foreign Policy Research Institute*, November 22, 2017, https://www.fpri.org/article/2017/11/three-little-oligarchs-latvias-corruption-scandal; Aaron Eglitis, "U.S. Sanctioning Russian Oligarchs Sparks Exodus of Cash From Latvia," *Bloomberg*, April 23, 2018, https://www.bloomberg.com/news/articles/2018-04-23/u-s-sanctioning-russian-oligarchs-spurs-cash-exodus-from-latvia; "Krisjanis Karins & Tambovskaya Mafia," *Lawless Latvia*, March 13, 2019, http://www.lawlesslatvia.com/2019/03/; "How Russian Oligarchs Turned the Country of Latvia into Their Own Personal Money Laundering Machine," *Gangsters Inc.*, August 3, 2016, http://gangstersinc.ning.com/profiles/blogs/how-russian-oligarchs-turned-the-country-of-latvia-into-their-own; "The KNAB Targets Latvia's Oligarchs," *The Economist*, June 8, 2011, http://country.eiu.com/article.aspx?articleid=218189406.

Then, the author started asking "Why" questions, hoping to find the root cause.

1. The first question was: Why is there vertical division in Latvian society? And the answer was relatively easy to find: *People distrust the political system*.
2. So, next "Why" question was asked: Why do people distrust the political system? The proposed answer, after an analysis, was: *The politicians do not take proper care of the people*.
3. Then came the next "Why": Why do the politicians not take proper care of the people? At that moment, there were several possible answers, which were rejected: *they are not qualified enough*, *they do not communicate with the society*, *they have bad advisors*, etc. Finally, it was decided that the best answer was: *The politicians*[67] *prefer to take care of their own business.*

   Next questions and answers, listed below, drove to the result that corruption can be the root cause:
4. Why do politicians prefer to take care of their own business?
   They have close connections.
5. Why do they have close connections?
   They merge business with politics.
6. Why do they merge business with the politics?
   They are corrupt.

But the author decided to continue as corruption also has a root cause, which should be found. The author decided to stop as this may have brought erroneous results, so after question number seven, there is no answer.

7. *Why are they corrupt*?

Future Implications

In the short-term, the Latvian government will probably decide how the next few years will develop for Latvia. The elections in October 2018 brought an end to the previous coalition of right parties. The Pro-Russian "Harmony" party got almost 20% of the vote, and the other two populist parties got respectively: "KPV" – 14 % and "New Conservative Party" – slightly below 14 %.

Despite some opinions, the high score of "Harmony" does not mean that Latvia may be turning towards Russia, as this party also has many Latvian members. Public support for this party has been decreasing: in 2011 – 28% of support, in 2014 – 23%, and in 2018 – slightly below 20% of support. So, the better results of the populist parties may mean that people simply got tired of the many scandals, corruption, and the lack of progress. The scale of change is significant, as only 1/3 of the current parliament will remain, while the new parties that will

[67] The three oligarchs are still active: one of them is a city mayor, the second is a businessman, and the third is a government official. Looks like one, closed circle, separated from ordinary people.

probably form the government will provide young inexperienced politicians.[68] Despite many changes, the defense and current security policy should remain unchanged – when Latvians were voting about the enhanced forward presence of NATO and expenditure of 2% of GDP for defense, all parties voted in favor. And there are plans to spend more if necessary.[69] There has been some speculation that Russia may try to influence "Harmony" or the future coalition of the populist parties against Latvian society. If this happens, it will probably employ reflexive control and try to exploit the gaps like vertical division (distrust of society towards the Latvian government), horizontal division (disparity between the Russian minority, which is facing language reform, and the Latvian population), and economic inequality, where people with low income and pensions strive to exist and survive (for example, Russian non-citizens). On the other hand, a possible conflict or crisis in Latvia or another Baltic country may not start by the incitement of the Russian minority. Creating a hostile attitude in the diaspora and then trying to destabilize the country from inside would take too much time and would give enough indicators for the government and NATO to react; only to mention the Estonian words "they may come, but they will meet fight at every corner" – and probably the same would happen in Latgale, for example. Instead, an invasion might be very fast and covert by the use of trains, for example.[70]

But this is unlikely because in October 2018, NATO's SACEUR Gen. Curtis Scaparotti, during a Military Committee meeting in Warsaw, discussed the whole-of-government approach as the reaction against any Russian hybrid warfare. He also stressed the fact that Russian coercion must be fought as a part of a unified effort because "nations themselves have different strengths, weaknesses, and vulnerabilities," and it is necessary to determine which threats will be dealt with by the use of the military, and which will require other countermeasures.[71] This seems to be addressing Latvia. When considering Russian activity, it is possible to speculate that Latvia has, indeed, experienced Russian coercion, for example in the military domain – the ZAPAD 17 exercise when Russian forces were visible literally on the border, in the internal domain – RBOC and the activity of Russian special services, and in the economy – the Russian footprint that exceeds 12% of GDP. So, if the gaps in Latvian society are closed, Russia will have difficulty in covertly entering the country.

In a long-term perspective, the demographic decline will hit Latvia hard. The decrease in the size of the population is of a catastrophic nature. The now scarcely populated areas will be depopulated even further and it may become a country of old people with huge economic disparities. The lack of young people (the brain drain) will also contribute to this gloomy picture, which raises such

[68] Interview with a Latvian government official, October 8, 2018.

[69] Interview with a Latvian government official, October 8, 2018.

[70] Interview with a Latvian government official, October 8, 2018.

[71] Samuel Cranny-Evans, "NATO Announces Plans to Counter Russian Hybrid Warfare," *Jane's Defence Weekly*, October 2, 2018, https://www.janes.com/article/83503/nato-announces-plans-to-counter-russian-hybrid-warfare.

questions as who will do the work and who will defend the country in the future. These are the questions that the government, no matter of which political persuasion, will have to swallow and digest. The remedy for this trend would be to bring the birth rate back to at least 2.2 to sustain the population and to try to reverse the emigration trend. As for the current Russian minority, it must be integrated into Latvian society because simply there is no alternative. The non-citizens diaspora will diminish, anyway, due to mortality and the naturalization of the youth. This will require a tough but open stance from the Latvian government towards Russia to fight derogatory messaging and fake news. Nevertheless, efforts are being made. In Latgale, for example, where Latvian TV transmitters presently lose their signal to more powerful Russian stations. Latvian TV stations are erecting transmitting stations and broadcasting Latvian-made Russian programs to communicate with the Eastern part of the country.

The Eastern flank of NATO will be continuously and aggressively tested by Russia, which will employ the strategy of raiding to try to weaken the Alliance. Russia has excelled at coercing other countries by indirect warfare. However, since the Baltic States, although directly exposed to Russian coercion, have shown themselves to be resistant, Russia may turn towards other possible targets on the Eastern flank, like North Macedonia, the Western Balkans, or even Hungary and Bulgaria.

But this process will also depend on the future shape and cohesion of NATO. Since Russia enjoys dealing with countries separately, not with a unified body, any crack in the allied relations will bring benefits for the Kremlin. That is why demands from the US towards the European partners about the necessity for bigger contributions to NATO are not only calls for bigger burden-sharing. This strategy will probably result in a more compact and more cohesive structure for NATO in Europe – "a return of European geopolitics." [72]

Conclusions

The presence of a Russian minority in Latvia, especially after the elections in October 2018, could be a good basis for Russia to undermine the country's cohesion. However, this matter should not be overstated, as this group is not homogenous. There are pro-Latvians and pro-Russians amongst this minority. Also, the picture concerning potential weak points in the Russian diaspora—compatriots and non-citizens—is not black and white. There are Latvian Russians who have distinct opinions about living conditions in Latvia and in Russia and do not believe in Russian propaganda and fake news. The Latgalians, in particular, should not be perceived as being a completely pro-Russian group. Amongst them there are both pro-Russian citizens and there are patriots who do not fear Russia and are

[72] Sten Rynning, "A Europeanized NATO? The Alliance Contemplates the Trump Era and Beyond," *War on the Rocks*, September 25, 2018, 12, https://warontherocks.com/2018/09/a-europeanized-nato-the-alliance-contemplates-the-trump-era-and-beyond.

ready to fight a bloody war.[73] However, though the Russian diaspora does not pose a threat *now*, if impelled from outside, for example by Russian coercion, it may react against Latvian society. It is also the conclusion that Russia, if it decides to intervene in Latvia, will not do it to protect the diaspora but will do it because of strategic choices, and the Russian minority will just be used as a tool.

Russian-based organized crime may emerge as one of the most effective and covert means of coercion in Latvia. It has been deep inside Latvian society since Soviet times and will be difficult to erase. Its existence should be analyzed together with its direct connection with the Kremlin, the Russian economic footprint and the problems affecting the Latvian banking system. In the future, if the Kremlin requests it, the RBOC will probably become heavily involved with Russian attempts to incite unrest, to corrupt politicians, and to gather information. The fight against this must be marshaled on both a national and an international level.

Russia has been practicing extensive, hostile, cross-domain coercion in Latvian living space, hoping to weaken the cohesion on NATO's Eastern flank. The most spectacular cases were the ZAPAD 17 exercise, cyber-attacks, the derogatory propaganda from state-owned TV stations, and the radicalization of the youth (radicalization camps).[74] These efforts may evolve into more aggressive measures, and even the use of direct warfare cannot be written off.[75] What is more, Russia is capable of using Belarus as a proxy against the Baltic States. The good news is that the self-esteem of the Latvian population is growing as people compare the information from different sources and question the fake news. This may also lead to another conclusion that Russian propaganda is becoming an obsolete tool, and Russia will then try to engage in other domains, probably cyber, which is both relatively cheap and very effective, and has no borders.

The Eastern flank of NATO has been tested for a long time, and this process will increase. The Russian effort may concentrate, apart from the Baltic States, on other "promising" targets, such as North Macedonia, the Western Balkans or even Bulgaria, where the Russian economic footprint makes state capture quite a realistic proposition. This research has found that the vertical and horizontal divisions in Latvian society are dangerous for national security. Social inequality is also a serious obstacle to Latvian society and national cohesion. The distrust towards the government is, unfortunately, justified in the face of corruption and political associations along with money laundering and social inequality, which is especially rife in rural areas. This pervasive phenomenon is of a very dangerous nature, as its existence, in the face of low social capital and demographic decline, creates permissive conditions that affect Latvian society in many domains. This

[73] Interview with a Latvian service member, October 8, 2018.

[74] This problem has been also mentioned by Latvian Security Police. See "Public Report on the Activities of Latvian Security Police," 8, 9,15.

[75] The case of Skripal shows the real intentions of Russia – for the Kremlin there are no borders that can stop its influence.

gap should be eliminated as soon as possible, as it works against the cohesion and resilience of Latvia.

There are areas which this study has found to be lacking in research, and the first would be the nature of Russian based organized crime in Latvia. In fact, there is not much information about it, maybe due to the fact that most data is classified. But its suspected ability to affect the Russian diaspora by physical coercion and intimidation and its direct link to the Kremlin may be disastrous if it is ever to be unleashed. There is evidence that, apart from money laundering, currently it is dealing with intelligence gathering for Russia, as well as cooperating with criminal groups on the border. This means that, despite the surprisingly positive resilience of the Russian diaspora in Latvia, Russia has the window and potential to covertly enter the country and exert cross-domain coercion from inside. Other areas that should be explored further include the current state of the Latvian population, the cooperation between the Baltic States in dealing with their Russian minorities, and the breakdown of the Russian minority in Latvia.

This study has touched on just a few aspects of Russian indirect warfare. There are other promising domains for research, such as cyberwarfare, the economy, or lawfare. Certainly, research into any of them could bring extensive results and some interesting conclusions for the future of NATO. But even at this stage, this work constitutes a very clear message that the cohesion and unity of a nation are of utmost importance when opposing cross-domain coercion.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Rosław Jeżewski serves in the Polish National Military Representative Office for NATO's Supreme Headquarters Allied Powers Europe operations in Belgium. He has a background in the Polish Navy and the Current Operations and Planning branches of the Polish Operational Command. He has been deployed to Ethiopia as a United Nations military observer and to Afghanistan as an advisor to the Afghan Army. His expertise includes demographic trends, migration, regional security and projecting stability. He is a graduate of the Marshall Center's Program on Applied Security Studies. *E-mail*: r.jezewski@ron.mil.pl.

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Mika Kerttunen, *Connections QJ* 18, no. 1-2 (2019): 61-68
https://doi.org/10.11610/Connections.18.1-2.04

Research Article

Beyond Punishment: Deterrence in the Digital Realm

Mika Kerttunen

Cyber Policy Institute, Tartu, Estonia, https://cpi.ee/

Abstract: Deterrence theory has since its inception justified the build-up and maintenance of weapons arsenals assumingly guaranteeing our survival. However, we do not know whether deterrence theory works in practice: major wars may have been avoided for many other reasons than fear of punishment or (other) high costs. Skepticism towards cyber deterrence is used to justify unilateral, punitive, even preventive, pre-emptive, or continuous action against assumed adversaries. Nuclear weapons-centric deterrence, stressing the avoidance of reckless state behavior, could be improved to face the contemporary, technology-infused realities, where zero-tolerance of error or incidents, vital in the nuclear realm, is not realistic. As a result, we have come to accept or denounce cyber operations based on their targets and effects. As a contribution to achieving responsible state behavior in cyberspace, the author suggests utilizing cost calculation, the underlying assumption of deterrence theory, to the fullest: to include the promise of rewards in our policy options.

Keywords: cybersecurity, deterrence, cyber domain, compliance, tolerance, attribution.

The Comfortable Laziness of Deterrence Theory

Can anything new and meaningful be said of deterrence? Not necessarily starting from Hermocrates of Syracuse, any analysis of deterrence has at least to notice that deterrence, narrowly understood, refers to a threat of punishment.[1] At the

[1] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960/1980); also Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966/2008); and Paul K. Davis, "Deterrence, Influence, Cyber Attack,

Creative Commons BY-NC-SA 4.0

same, it should be noted that a wider reading acknowledges two aspects of deterrence: punishment and denial. Moreover, it is appropriate to table the latest interpretation, specially tailored for cyber affairs, which adds in the aspects of entanglement and normative taboos.[2]

Intellectual analysis starts with references to the logic of deterrence. Firstly, that at the core lies the pure assumed logic, or law, of economics. A rational actor is a calculative creation who knows what to choose: a lower cost (Formula 1).

Cost of compliance < *Cost of non-compliance*

Formula 1. The pure economic logic of being deterred.
(author's compilation)

Regardless of what is assumed to cause the deterring effect—abstaining from thought behavior: pain, failure, rewards, accumulation of costs, or shame—the theory, or the theories, assumes the adversary being belligerent, but, despite that, to act rationally, basing his or her decision-making on calculation, weighing the totality of potential while considering the likely costs and gains.[3] Secondly, it does not hurt to mention Schelling's fundamental thesis of the bargaining power of *harm versus no harm*:

> But suffering requires a victim that can feel pain or has something to lose. To inflict suffering gains nothing and saves nothing directly; it can only make people behave to avoid it. The only purpose ... must be to influence somebody's behavior, to coerce his decision or choice. To be coercive, violence has to be anticipated. And it has to be avoidable by accommodation. The power to hurt is bargaining power. To exploit it is diplomacy – vicious diplomacy, but diplomacy.[4]

Finally, one has to acknowledge the limitations of deterrence. Deterrence theory—and most importantly, its credibility—assumes resemblance between the imposed threats, the values of the adversary, and the anticipated rational behavior. Deterrence, as a principal political commitment, is absolute, yet real-life choices and the operationalization of deterrence call for challenging value

and Cyber War," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. For Hermocrates of Syracuse, see Thucydides, trans. Martin Hammond, *The Peloponnesian War* (Oxford: Oxford University Press, 2009).

2 Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.

3 Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961).

4 Schelling, *Arms and Influence*, 2.

choices.[5] How much, for example, harm, cost, or pain is needed, and what constitutes cost, pain, or shame?

And how does the Other know of our capacity and of the calculations we have taken on his/her behalf? Communication is imperfect, and perfect understanding impossible. Moreover, there is an asymmetry of information. For example, while it is safe to assume that the attacker has fairly sufficient knowledge of the targeted cyber system and the values associated with it, the defender is not necessarily aware of the attacker's identity or strategy or payoffs. Moreover, the cyber defender may be forced to act only at certain points in time, while the cyber attacker is free to become active at any time. This is emblematic of the dilemma between *discrete time* for one player and *continuous time* for the other.[6]

Regarding cyberspace, it is appropriate to notice that deterrence in cyberspace is challenging or does not function at all. The very fact of malicious cyber operations taking place is hard to establish. Further evidence comes from the stealthy, speedy, or non-attributable nature of cyber activities, which often are conducted by non-state actors, or that there are no appropriate means or political-legal frameworks to punish the cyber-perpetrators.

In fact, the very claim that deterrence functions cannot be verified or falsified. The very deterring effect is a cognitive one. Deterrence theory, albeit often loaded with calculations, cannot explain or predict any behavior; at best, it is *an ideal or hypothetical set of facts, principles, or circumstance,* or simply, *an abstract thought*.[7]

Accordingly, the study of deterrence has become studies of certain elements considered to be essential in the established canon of deterrence. Moreover, skepticism towards cyber deterrence is used to justify unilateral, punitive, even preventive, pre-emptive, or continuous action: since deterrence does not work in cyberspace, it is responsible for taking action and causing costly effects to the alleged Other, especially as there is no threat of annihilation by retaliation. This

---

[5] Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica, CA: RAND, 2017), 21–22, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf; Andrew Higgins, "Two Border Cities Share Russian History – and a Sharp European Divide," *The New York Times*, November 9, 2017, https://www.nytimes.com/2017/11/09/world/europe/narva-estonia-ivangorod-russia.html.

[6] Kien C. Nguyen, Tansu Alpcan, and Tamer Basar, "Security Games with Incomplete Information," in *Proceedings of the 2009 IEEE International Conference on Communications*, 14-18 June 2009, Dresden, Germany, https://doi.org/10.1109/ICC.2009.5199443 (studying the game theory of security games and discrete time); Stefan Rass, Sandra König, and Stefan Schauer, "Defending Against Advanced Persistent Threats Using Game-Theory," *PLoS ONE* 12, no. 1 (2017), https://doi.org/10.1371/journal.pone.0168675.

[7] *Merriam-Webster English Dictionary.*

belief is based on a limited understanding of cyber deterrence. Despite its narrow, formal correctness, it is dangerously wrong.[8]

We simply do not know if deterrence actually works or not. This uncertainty, together with the fact, claim, or assumption that with the cyber condition we have entered at least partially a new operating environment, calls for a new narrative of deterrence.

A New Narrative of Deterrence: Four Claims

Changed Context

Although the logic of deterrence could be traced to general and ancient human behavior, the genealogy of deterrence theory is conditioned by the bipolar Cold War. Then the double-intent of the two superpowers can be said to have sufficient power to destroy the other while ensuring the survival of human life on the planet. The concept of deterrence allowed to justify the former and to assure of the latter.

Nuclear weapons and the superpower ability to destroy the planet has not disappeared. Yet, the conditions and the context of cyber deterrence are different. Whereas previously deterrence stressed the avoidance of reckless state behavior, the contemporary cyber discourse focuses on responsible state behavior. Deterrence, as we have come to know it, does not seem appropriate or credible.

Wider Tolerance

Moreover, whether in the nuclear setting, in the Cold War and now, the culture of zero tolerance prevailed. Failures of deterrence, at least in the purest sense, would have been unacceptable. A nuclear or any major military attack would have been met by countermoves, even retaliation, when everything had already been lost.

In cyber affairs, nobody could live with zero tolerance. Information and communications systems are inherently vulnerable, prone to technical incidents or human errors, let alone deliberate attacks. In fact, if during the Cold War superpower military confrontation was acceptable in the global periphery—Asia, Africa, and Latin America—we have now come to have three *de facto* layers of acceptance of cyber operations.

Readily accepted are operations conducted by intelligence agencies, security and law enforcement organs and armed forces against universally recognized extremist, terrorist or criminal organizations since, fo example, the United Nations Security Council (UNSC) Resolution 1373 (2001) determines all forms of ter-

[8] Similarly wrong is to uncritically assume that cyber activities are invisible, fast and non-attributable. Any analysis beyond airport literature can notice the tangible effects and the months and years of preparation of cyber-attacks, and the official attributions made to state and non-state actors. The speed of light, as well as the speed of a bullet or a fighter plane, are very poor indicators to inform of the speed of an attack, operation or campaign.

rorism as constituting a threat to international peace and security. Therefore, it is relatively easy for the international community to accept, even hail, the US offensive military cyber operations against the "Islamic State." On the other hand, state cyber operations within existing dyadic conflicts or against lower value targets, hypocritical or not, are contingently accepted. For example, Israeli cyber operations against the Syrian government, or Hezbollah, do not trigger international objections beyond the usual – but the US ones against the very same targets would. The alleged Dutch intelligence agency operation infiltrating to Moscow State University systems[9] did not make any waves, maybe because states are reluctant to problematize intelligence activities they all are conducting, and maybe because the target of the operation was (said to be) a Russian origin cyber-criminal grouping. Operations which seem to be unacceptable are ones that properly jeopardize the international order or national security. Therefore, operations such as the 2016 infiltration into the Democratic National Congress servers and exfiltration of data or the 2017 attempt to hack the Organisation for the Prohibition of Chemical Weapons are considered dangerous and irresponsible, receiving wide international condemnation.

Obviously, this factual tolerance of cyber operations challenges the established logic of deterrence: they are incompatible. The very absence of any serious cyber operation rather witnesses either of states' inability or their caution to conduct such effect-creating and profound operations in peacetime than of deterrence. Yet, the practice of cyber operations by exploiting the thresholds of use of force and armed attack challenge international law and, most seriously, the rule of law many of the keen operations verbally are endorsing.

More Approaches

Conceptually, and borrowing from ancient Chinese thinking, deterrence by punishment is a negative approach and deterrence by denial – a neutral one. As we are being told, the former seeks actively to reduce the bad actor's values, and the latter denies any increase in those values. If the rational man's calculative logic is correct, as it is assumed, then offering rewards should also deter an actor from taking action he would otherwise take – positive deterrence: deterrence by benefits.

Such benefits can be created in several ways. Mirroring the concept of deterrence by punishment, deterrence by benefits could reward certain behavior of states. Taking into account the concept of deterrence by denial, it could feature the development of infrastructure, cooperation models, exchange of know-how, or the setting of plurilateral, sub-regional, or other common goals that leverage the economic and social benefits of information and communication technologies. Benefits can also be achieved, in the context of entanglement, as a result

[9] Rick Noack, "The Dutch Were a Secret U.S. Ally in War against Russian Hackers, Local Media Reveal," *The Washington Post*, January 26, 2018, www.washingtonpost.com/news/worldviews/wp/2018/01/26/dutch-media-reveal-country-to-be-secret-u-s-ally-in-war-against-russian-hackers/.

of reduced expenditure and optimization of costs by way of joint reduction of cyber risk. Furthermore, the anticipated benefits could be improved reputation, ranking in relevant international venues or assessments, or acknowledged leadership in international processes. Compared to the normative taboo and the zero-tolerance tools, deterrence by benefits would emphasize maximizing common benefits and therefore full support and universal acceptance/endorsement of certain behavior.

It is further hypothesized that the classical theory of deterrence no longer satisfies states' political ambitions sufficiently. Especially in Europe, there is a strong hesitation towards hard-security deterrents, including sanctions and countermeasures imposed under, and especially in the outskirts of international law. Instead, states are increasingly interested in economic and social incentives behind the behavior of their counterparts.

A key criticism towards deterrence by punishment is the fact that wherever punishment becomes actionable, deterrence has, by definition, failed. Accordingly, in the case of benefits, the anticipatory and preventive nature of deterrence is maximized. It can also be argued that deterrence by benefits maximizes reciprocity and, therefore, promises the widest possible platform of shared interests and universal acceptance of certain behavioral modalities. By enhancing the study of changing the calculus of malicious or hostile acts, states could increase the return of security investments. It is presumed that a reduced margin of politico-military risk also lowers forced defense and military expenditure while adding to the social and economic budget that creates resilience and strengthens the information society.

Investments into resilience and good security practices, in turn, are likely to significantly increase the cost of bad behavior, therefore creating additional denial thresholds. In this context, resilience as an actor-neutral measure is emphasized and promoted.

Nuanced Tools

States or groups of states should thus look beyond sanctions, or the negative aspects more generally. Indeed, we should recognize how well resilience as implicit deterrence by denial works: the number of effect-creating cyber operations is very small, especially compared to cybercrime and common talk of cyberwar being waged.[10] Actually, the very extent of cybercrime testifies of the insufficient governmental and organization investments in the capacity needed to deny cybercriminals from achieving their objectives. Moreover, national and international cybersecurity policies should incorporate positive agendas with rewards.

[10] Eneken Tikk, Kristine Hovhannisyan, Mika Kerttunen, and Mirva Salminen, *Cyber Conflict Fact Book: Effect-Creating State-on-State Cyber Operations* (Jyväskylä: Cyber Policy Institute, 2019). This analysis is based on the publicly known state cyber operations the Council of Foreign Relations "Cyber Operations Tracker" and other databases had gathered.

Conclusion

As we have come to know, deterrence is a cumbersome and inappropriate tool to understand the cyber realm. The conditions of the cyber condition and the new genealogy of deterrence are different from and far more nuanced than those of the nuclear setting.

As technological, political, and societal parameters and premises are different; therefore, the conclusion is too. Cyber deterrence to function as a cybernetic steering mechanism of state behavior needs paradoxically be built on the acceptance of error and incidents as well as low-intensity attacks. This acceptance draws lines between tolerable and intolerable. We, the West, have to ensure that the standards of responsible state behavior become as high as possible. Our eagerness to exploit our technological supremacy and conduct cyber operations should not undermine the rule of law and higher moral ground. Since deterring an actor is both theoretically questionable and, in the cyber realm, practically not feasible, sanctions of all kinds are to create state practice and boundaries of responsible/irresponsible state behavior.

Managing the new setting of uncertainty, blurred lines of responsibility, the many thresholds, and the many actors cannot solely rely on the black-or-white logic of the negative, i.e. punishment. Resilience should replace punishment and caution brinkmanship in our strategic lexicon. Robust (national) resilience as threat-neutral and de-escalatory is also better suited to accommodate unpredictability, a feature particularly relevant to the cyber context, than deterrence, or persistent engagement for that matter. The success of the dominating risk and threat (actor) based approaches, or both deterrence and persistent engagement, being conditioned by the accuracy of the (pre-) assessments is in itself too risky.[11] The West has to incentivize responsible behavior in cyberspace. Resilience and rewards coupled together create a powerful and peaceful policy option no other state or group of state can offer. The negative alone is insufficient.

Thus, in the new formula (Formula 2 below) of being deterred the law of economics still rules, but costs are replaced by rewards.

[11] Gerard de Vries, Imrat Verhoeven, and Martin Boeckhout, "Governing a Vulnerable Society: Toward a Precaution-Based Approach," in *Vulnerability in Technological Cultures: New Directions in Research and Governance*, ed. Anique Hommels, Jessica Mesman, and Wiebe E. Bijker (Cambridge, MA: MIT Press, 2014), 225. The referred chapter is based on the report *Uncertain Safety* which the Dutch Scientific Council for Government Policy (WRR) has adopted as official advice to the Dutch cabinet. Risk management adopted, or at least cited, in many national cybersecurity strategies, seeks to identify and evaluate risks in terms of probabilities and extent of damage and design and take measures to limit or control those risks considered unacceptable.

Rewards of compliance > Rewards of non-compliance

Formula 2. The new economic logic of being deterred.
(Author's compilation)

This turn does not assume the almost automatic bellicosity of the Other. We thus avoid the illusion of deterring the Other in a situation where such bellicosity is not necessarily being considered taking. Instead, we focus on the more likely motivation and ambitions governments have – positive rewards. Obviously, a leader determined to go to war will not be turned away by threat of punishments, anticipated hardships, or benevolent rewards.

Such a turn in thinking would not be appreciated by the security – cyber-industrial complex riding on the threat and promise of an apocalyptic future. For the rest of the humankind preferring peace, prosperity and global justice such turn would make sense.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

LTC (ret., Finish Army) Mika **Kerttunen**, D.Soc.Sc. (Pol.), is Director of Studies, Cyber Policy Institute (Tartu, Estonia). He is a graduate of the Finnish Military Academy and General Staff Officer Course as well as the Royal Norwegian Command and Staff College. Kerttunen studied world politics at the University of Helsinki and analysed in his 2009 dissertation Indian foreign and nuclear policy. After his military service he has been focusing on cyber issues in foreign and security policy, the development of cyber norms, and the development of national cyber security strategies and military cyber doctrines. Dr Kerttunen is advisor at the Finnish delegation at the UN Group of Governmental Experts on Information Security (2016-2017) and Visiting Faculty Member at the University of Tartu Law School.

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Manuel Fischer, *Connections QJ* 18, no. 1-2 (2019): 69-92
https://doi.org/10.11610/Connections.18.1-2.05

Research Article

The Concept of Deterrence and Its Applicability in the Cyber Domain

Manuel Fischer

George C. Marshall European Center for Security Studies,
http://www.marshallcenter.org

Abstract: Cyberspace as the fifth domain is omnipresent, and all developed states increasingly realize that international relations and typical domains of statehood change in the face of global digitization. With the advent of game-changing technologies, traditional statecraft tools, such as deterrence, seem disregarded as outdated in the national security strategy building process. Advanced states, in particular, depend heavily on an open and safe cyber domain but, at the same time, suffer from manifold vulnerabilities. The recent past showed that sophisticated cyberattacks have the potential to disrupt governments, economies, and societies significantly and therefore pose a threat to core security interests. As a classical tool in international relations, deterrence can help bolster national security interests, even if the cyber domain requires some special considerations. Therefore, the article explains the basic mechanisms of deterrence in the nuclear age and contemporary international relations, cyberspace's legal framework, and possible ways to apply deterrence in the cyber domain. It aims to urge global leaders to thoroughly consider deterrence in the cyber domain as a powerful asset and to provide policymakers with options for action.

Keywords: cybersecurity, cyber operations, deterrence, legal framework

Introduction

Speaking about deterrence in the 21st century feels like excavating remnants of a bygone era. With the advent of nuclear technologies and mainly during the Cold war, deterrence was a topic not only for politicians and academia but also shaped the daily lives of millions, no matter which side of the 'blocks' they belonged to. Since then, deterrence diminished its presence in the public percep-

Creative Commons BY-NC-SA 4.0

tion together with the nuclear arsenals of the great powers. What remains is still of enormous potential but as a tool of statecraft rather than a placeholder.

Especially states face the gradual change of the traditionally state-centered setting of the international system, particularly in habitual domains of statehood, like security. The classical understanding of war and conflict blurs and the traditional state structures seem to be overstrained to respond with the classical tools, as the new type of conflict is multilayered (political, military, and economic, among others), conducted mostly by non-military means like propaganda and political agitation and amongst diverse state and non-state actors.[1,2]

In the face of daily and continuing attacks on governments and their organs,[3] the question persists: What keeps an actor in the cyber domain from carrying out the same attacks over and over again, or even climbing up the escalation ladder and causing irreversible harm, if it serves his interests. There seems to be no respect, no fear of retaliation, and no serious technical barriers in the cyber domain – or in other words, no deterrence.

This article will survey if the concept of deterrence is only effective if it is tied to nuclear weaponry and if it becomes useless in a no longer (purely) nuclear but cyber-dominated international system. The author claims that this is not the case! Even in the cyber age, deterrence can be a powerful tool of statecraft and could contribute to the protection of state's national security interests. To prove this hypothesis, this article will scrutinize the concept of deterrence by looking into the past that generated manifold experiences on that topic, to finally project the findings into present times. Therefore, existing concepts of deterrence and special implications of the cyber arena, together with the legal framework of the ever more digitized international system, will be examined to finally find effective ways to apply deterrence in cyber space.

---

1 David J. Betz, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (London and New York: Routledge, 2017), 80.

2 Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, quote on p. 48, https://doi.org/10.1162/ISEC_a_00266.

3 Like it happened in Germany in 2015, when a Russian hacker group called "Fancy Bear" attacked the German Parliament, spied on at least 16 members (including Angela Merkel) and extracted several partly confidential documents. By that time, the Federal Chancellery spoke about (hybrid) warfare and potential counterstrikes for the first time since decades. See Patrick Beuth, Kai Biermann, Martin Klingst, and Holger Stark, "Bundestags-Hack – Merkel und der schicke Bär," *Zeit Online*, May 10, 2017, http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland. And yet, the same happened again in late 2017, when security officials detected a presumably Russian originated "Advanced Persistent Threat" aimed at the foreign ministry, which compromised the network for up to a year. See Thorsten Severin and Andrea Shalal, "German Government under Cyber Attack, Shores up Defenses," *Reuters*, March 1, 2018, https://www.reuters.com/article/us-germany-cyber/german-government-under-cyber-attack-shores-up-defenses-idUSKCN1GD4C8.

The following assumptions and exclusions are considered common ground:

- The emerging fifth-generation mobile technology (5G) and cloud technologies will boost the spreading of the Internet of Things. Critical processes will be gradually transferred to these technologies and cyber risks will rise exponentially as the new devices create more opportunities for potential breaches. Plus, by controlling physical assets, even physical harm can be caused.[4,5]
- According to the "Assume-Breach-Paradigm," it is highly likely that every sufficiently complex software product has critical vulnerabilities and that updates are either not provided or the vulnerability is kept secret.[6]
- This research will focus on political cyber threats and cover criminal cyber activities only as far as they occur in the context of conflict. Traditional espionage via cyber means will be excluded from this research.

Mechanisms of Deterrence

The concept of deterrence is as old as mankind's craving for fighting each other.[7] The term "deterrence" is derived from the word "terror," which reflects the fear of costs that are related to a certain action. In academic literature, sometimes the term "dissuasion" appears to indicate the broader range of measures, which are not only focused on inflicting costs but also on denying benefits for the adversary.[8] For the sake of a clear distinction and in view of the dominating use in the political and academic realm, this work will use "deterrence" as an umbrella term, aware of the fact that the concept is much broader.

Joseph Nye also takes both denotations into account by defining deterrence as[9]

> … dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit.

---

4 "BSI: Critical infrastructures – Definition," Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance, 2017, www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html.

5 James Manyika, et al., *The Internet of Things: Mapping the Value beyond the Hype* (McKinsey & Company, June 2015), 11.

6 "BSI: Critical Infrastructures," 18.

7 Early references date back to Thucydides' work about the Peloponnesian War, even before the Christian calendar emerged, see Richard Ned Lebow, "Thucydides and Deterrence," *Security Studies* 16, no. 2 (2007): 163–188, quote on p. 163 https://doi.org/10.1080/09636410701399440.

8 Michael Quinlan, "Deterrence and Deterrability," in *Deterrence and the New Global Security Environment*, ed. Ian R. Kenyon and John Simpson (London: Routledge, 2006), 5.

9 Nye, "Deterrence and Dissuasion in Cyberspace," 45.

This means to preserve the status quo by preventing an opponent from conducting a course of action that is viewed as unfavorable. It is not about compelling the adversary to certain behavior and thereby altering the status quo.[10] Considering key mechanisms and the application in International Relations (IR) will help to understand the common ground and lead the way to cyber deterrence.

According to the deterrence theorists Sir Michael Quinlan,[11] there is "no such thing as an undeterrable state."[12] As basic prepositions for successful deterrence (no matter in which realm), he considers the following five points[13]:

1. Probabilities
2. Capability and a credible intent
3. Deterrence declaration
4. Prospect to cause multifaceted costs
5. Using the whole range of possible responses.

Probabilities

Ideal deterrence would work with certainties, for example, "if you take my lunch, I will destroy your toy." But as human interaction is of a rather complex nature, several uncertainties emerge, and misperception and misinterpretation are unavoidable. To face that, probabilities need to be considered.[14] Not only the potential gain value ("lunch") and loss value ("toy") play a relevant role, but also the probability of succeeding or losing. As a consequence, the dimensions of gain probability ("you can't be sure to get my lunch because I will try to defend it") and loss probability ("if you take my lunch, I will do my best to destroy your toy and maybe I will succeed") need to be added to the following decision calculus[15,16]:

*Gain Value * Gain Probability < Loss Value * Loss Probability*

---

[10] Wyn Q. Bowen, "Deterrence and Asymmetry: Non-state Actors and Mass Casualty Terrorism," *Contemporary Security Policy* 25, no. 1 (2004): 54-70, https://doi.org/10.1080/1352326042000290506.

[11] Former Permanent Under-Secretary of State at the British Ministry of Defense; influential defense and deterrence strategist.

[12] Quinlan, "Deterrence and Deterrability," 7.

[13] Quinlan, "Deterrence and Deterrability," 4.

[14] Quinlan, "Deterrence and Deterrability," 4.

[15] Philip Bobbitt, *Democracy and Deterrence: The History and Future of Nuclear Strategy* (Basingstoke: Palgrave Macmillan, 1988), 8.

[16] Jeffrey R. Cooper, "A New Framework for Cyber Deterrence," in: *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Georgetown University Press, 2012): 105-120, 109.

An effective deterrence in an uncertain environment needs to address all four factors of the inequation to ensure that the left part stays smaller than the right part in the adversary's perception.

Capability and a Credible Intent

Capabilities are the basis for an adversary to calculate the value he could gain and lose. However, there is also a need for a credible intent of using these capabilities to affect the calculation of probabilities.[17] Powerful offensive measures can increase the loss value, the credibility of offensive and defensive measures can change the calculation of probability of gain and loss.

*Gain Value * Gain Probability (↓) < Loss Value (↑) * Loss Probability (↑)*

Whereas capabilities are rather a matter of money, a credible intent can only be proven by action, but still, both need a "show of force" to be perceived by an opponent.[18]

Deterrence Declaration

Besides capability and credibility, the effective communication of the right deterrence message to the right audience is of significant importance.[19,20] Therefore, it is vital to state what actions will not be allowed to stand, that (offensive or defensive) capabilities for an appropriate reaction are at hand and that these will be employed.[21] Hereby, an over-exact, self-limiting specification is unnecessary and can even be detrimental, as it opens the path for the adversary to evade or head off a response.[22] Effective communication gives the adversary distinct factors for his calculation and reduces misinterpretations or misperceptions. Furthermore, a strong deterrence declaration can per se affect the perception of gain and loss probability.

---

[17] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham, Maryland: Rowman & Littlefield, 2017), 9.

[18] The US showed a new capability in the 1989 invasion of Panama by employing the F-117 Stealth fighter-bomber, surely not because of the threat of the Panamanian air defenses but to demonstrate a new capability in the toolbox, see Richard A. Clarke and Robert K. Knake, *Cyber War: What It Is and How to Fight It* (New York: HarperCollins, 2010), 194.

[19] Bowen, "Deterrence and Asymmetry," 51.

[20] Jasper, *Strategic Cyber Deterrence*, 9.

[21] Although a defined red line is missing, the U.S. provides a good example by publicly asking IT-contractors to compete for a nearly $ 500M contract to develop and, if necessary, deploy lethal cyber weapons. The executive director of U.S. Cyber Command stated that the U.S. is looking for loud offensive cyber tools that can be traced back to the United States. See Jasper, *Strategic Cyber Deterrence*, 102.

[22] Quinlan, "Deterrence and Deterrability," 4.

*Gain Value * Gain Probability (↓) < Loss Value * Loss Probability (↑)*

Current experts, like the former US undersecretary of defense for policy, James Miller, point out that, "[y]ou don't really deter states, you deter individuals and group decision-makers…"[23] This means that the deterrence declaration needs to be designed reversely, starting with the desired effect, and considering how it will be processed by those it should deter.[24] The assumption that an adversary acts rationally is rather simplified, as it would require perfect information and the willingness to take decisions only based on its strategic implications. Decision-makers never have perfect information and are influenced by many factors like emotions or personal interests.[25]

Prospect to Cause Multifaceted Costs

By building up defensive structures, the desired effect can be denied or at least mitigated. This will sow the seed of doubt in the adversary's mind as he needs more time and resources, and the probability of detection rises.[26] In short, denial measures increase the opportunity costs of the challenger. Combining retaliation and denial measures and increasing the variety of costs makes it harder for the opponent to prepare and harden its values in advance.[27] Thus, both the loss value and the loss probability rise.

*Gain Value * Gain Probability < Loss Value (↑) * Loss Probability (↑)*

To increase this effect, it can be expedient to tailor a strategy to a specific adversary. This demands contextual knowledge of the actor's motives, decision-

[23] Sean D. Carberry, "Why There's no Silver Bullet for Cyber Deterrence," *Federal Computer Week (FCW)*, June 06, 2017, https://fcw.com/articles/2017/06/06/carberry-cyber-deterrence.aspx.

[24] How an opponent interprets a deterrence declaration depends on their history and strategic culture and is a source of misinterpretation based on different preferences and expectations. See James Andrew Lewis, "Rethinking Deterrence," Report (Washington: Brzezinski Institute on Geostrategy, May 2016), 5, https://csis-website-prod.s3.amazonaws.com/s3fs-public/170713_Deterrence_Stability_0.pdf.

[25] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–135, 107, https://www.hsdl.org/?view&did=18663.

[26] Bowen, "Deterrence and Asymmetry," 50.

[27] Such a combination of retaliation and denial aspects was to be seen under the George W. Bush administration for deterring the use of unconventional weapons by regimes of concern through combining denial capabilities (development of a comprehensive missile defense) and the threat of overwhelming punishment. See Bowen, "Deterrence and Asymmetry," 50.

making processes, and command and control structures and would mean a high intelligence effort and cultural understanding.[28]

Using the Whole Range of Possible Responses

If the costs displayed do not match the means or magnitude of the actions attempted to prevent, even opponents of different sizes and value-systems can be deterred.[29] Using the entire range of possible responses makes it harder for the adversary to predict an answer and protect himself. Thus, the loss value, as well as the loss probability, can be increased.

*Gain Value * Gain Probability < Loss Value (↑) * Loss Probability (↑)*

As a state usually holds the monopoly on the use of force and possesses a wide range of kinetic means, this can be an advantage in facing non-state opponents. Switching the domains of response to classical and familiar grounds of statehood can strengthen legitimacy and credibility.[30]

Special Implications of the Cyber Domain

Ever since states and governments engaged with each other in the arena of IR, deterrence used to be a valuable tool. The most influential era of deterrence emerged with the advent of nuclear weapons and essentially defined the Cold War course. There are parallels to the cyber age, which can provide valuable help, but there are also aspects that must be disregarded.

The 1945 atomic bombing of Hiroshima and Nagasaki suddenly forced the world to face a new military capability that was perceived as unstoppable and producing non-survivable effects. It took strategists several years to come from NATO's so-called "massive retaliation" over the turning points of the Sputnik-Shock and the Cuba-Crisis and the subsequent deterrence concept of "mutual assured destruction" to the comprehensive strategy of "flexible response." That was a graduated concept, escalating from conventional defense to the strategic employment of nuclear weaponry. It was based on capability (conventional and nuclear forces) and at least some credibility (the US nuked Japan), relying on the whole range of means (from conventional response to tactical and strategic nuclear means) to promise multifaceted costs (strikes against military and eco-

[28] Bowen, "Deterrence and Asymmetry," 51.

[29] Quinlan, "Deterrence and Deterrability," 4.

[30] When the Islamic State's propaganda machine became too strong and uncontrollable, the U.S. government turned to lethal force in the shape of air-strikes against high-level media division operatives which became legitimate targets in an armed conflict due to their affiliation with the terrorist group. See Jasper, *Strategic Cyber Deterrence*, 95.

nomic targets on the battlefield and in the homeland), but it was not self-limiting in the ways of response (no predefined escalation-ladder).[31]

This well-defined strategy indeed brought a certain stability to the international system and was based on five factors that characterized the then modern concept of war (and thus of deterrence) in the face of new and complex technology[32]:

1. *Time factor:* Excessive harm could now be done in a short time, with hardly any prewarning.
2. *Force factor:* Immediately available forces outrivaled mobilization forces due to the time factor.
3. *Survival factor:* A first excessive strike needed to be survived to launch a counter attack.
4. *Globalization factor:* A nuclear war would escalate globally immediately.
5. *Defense factor:* NATO's defense needed to be based on displaying strengths, not on protecting weaknesses.

NATO is still a nuclear alliance (mainly based on the US capability and credibility), and nuclear deterrence remains a part of its defense strategy. Nonetheless, since the Cold War, the world's atomic arsenals got systematically reduced, and various non-nuclear technologies emerged. Some even say that in the context of powerful alternatives, nuclear weapons are relegated to a passive and symbolic role in IR.[33] At the same time, the vertical[34] and horizontal[35] proliferation of destructive technologies became easier to conduct and harder to control.[36]

But even if the concepts of nuclear deterrence cannot be copied, it is still possible to learn how a complex strategy for the use of new and overwhelming

---

[31] "Nuklearstrategie – Zwischen Abschreckung und Einsatzdoktrin," *Bundeszentrale für politische Bildung*, https://sicherheitspolitik.bpb.de/m6/articles/nuclear-strategy-between-deterrence-and.

[32] Bruno Thoß, *NATO-Strategie und nationale Verteidigungsplanung: Planung und Aufbau der Bundeswehr unter den Bedingungen einer massiven atomaren Vergeltungsstrategie 1952 bis 1960* (München: Oldenbourg Verlag, 2006).

[33] Lewis, "Rethinking Deterrence," 5.

[34] Increase in number and sophistication of weapons of established weapon holders. See Ian R. Kenyon and John Simpson, eds., *Deterrence and the New Global Security Environment* (Abingdon: Routledge, 2006).

[35] Dissemination of nuclear technology to others. See Kenyon and Simpson, *Deterrence and the New Global Security Environment*.

[36] In fact, the established nuclear powers are concerned that their nuclear deterrence might be circumvented or beheaded by advanced conventional weapons. These would not reach the nuclear threshold and thereby a strike of the level of a nuclear attack against vital values could stay unpunished, See Lewis, "Rethinking Deterrence," 4.

technologies can be developed.[37] In parallel with the nuclear age, the cyber age stands for the development of a new, man-made, and hard to grasp technology that has overwhelming potential for civil use and, at the same time, for unimaginable destruction. These common features enable the assumption that the same factors as in nuclear deterrence play at least a basic role in cyber deterrence. The following paragraph will examine the previously introduced implications of time, forces, survival, globalization, and defense in the cyber domain and will add the cyber specific factor of attribution to the set of aspects.

Time Factor

In the cyber age, the time factor for the attack itself seems to tend to zero as Artificial Intelligence employs algorithms to take over basic, but time-consuming tasks, and actors all around the world are connected in milliseconds. This so-called "net-speed" creates a simultaneity of cause and effect that ceases the need to costly and difficultly bridge distance. Now even small actors can affect states without any prewarning.[38] However, this only holds true for the attack itself. Similar to the Cold war, the preparation of the battlefield is a necessary precondition to attack in net-speed. Like identifying command bunkers, an advanced cyber attacker needs to infiltrate and map a system, gain access and place backdoors.[39,40] This means a long-term campaign, which cannot be conducted entirely from behind a computer but consists of complex human intelligence (HUMINT) operations.[41]

Force Factor

Immediately and constantly available forces with the latest technological knowledge and equipment outrivaled mobilization forces due to the time factor. Still, governments use the same concepts as for noncyber attacks by delegating defensive tasks and deterrence duties against small actors to local police forces and employing federal agencies only against state actors or terrorist groups.[42] This means fragmentation of responsibilities and an incoherent strategy. Simultaneously, technological knowledge and equipment cost immense amounts of money and require agile and specialized structures. Both are only available to a

---

[37] Clarke and Knake, *Cyber War: What It Is*, 155.

[38] Betz, *Cyberspace and the State*, 39.

[39] Richard B. Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 89–104.

[40] Clarke and Knake, *Cyber War: What It Is*, 30.

[41] Jeffrey Carr, "Responsible Attribution: A Prerequisite for Accountability," Tallinn Paper No. 6 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014).

[42] Andres, "The Emerging Structure of Strategic Cyber Offense," 91.

certain extent in governments, and therefore an increasingly significant role falls to the private sector.

Special focus falls to the supply chain of IT soft- and hardware. Often cybersecurity and data protection issues are not considered in the invention stage and the ex-post fixing of vulnerabilities is not always possible.[43] By compromising hardware in an early stage of development, vulnerabilities can be created and easily distributed up the supply chain.[44] This brings into focus the whole chain, down to the smallest "smart valve." Although such targets may sound insignificant, it has been evaluated that especially highly sophisticated threat agents concentrate on them.[45] Thus, it has become crucial to determine who manufactures, tests, and certifies hardware, where spare parts come from, and which manufacturing and distribution processes need to be under constant national control.

Survival Factor

Being able to survive the first strike and staying able to act was a key element in the nuclear setting. The cyber domain as well seems to be an offence-dominated environment in which attackers have a structural advantage over defenders, and definite protection is not possible. Moreover, industrialized and connected countries seem to be more vulnerable than less advanced ones.[46,47] This leads to a nuclear-era-like self-deterrence of the powerful, industrialized, and connected states. Being aware of their own cyber vulnerability, a reluctance to use the usual superiority in other areas (like conventional weapons) emerges.[48] As it seems impossible to reduce the level of interconnectedness in modern societies, the best option is to improve deterrence and defenses.[49]

---

[43] ENISA, "Threat-Landscape-Report 2017" (Heraklion: European Union Agency for Network and Information Security), 107, www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport.

[44] This phenomenon is not exclusively linked to the cyber domain. For years, the U.S. Department of Defense (DOD) struggles with counterfeit parts in its critical defense supply chains. See United States Government Accountability Office (GAO), "Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk" (Washington D.C.: US GAO, 2016), https://www.gao.gov/products/GAO-16-236.

[45] ENISA, "Threat-Landscape-Report 2017," 110.

[46] Jack L. Goldsmith, "How Cyber Changes the Law of War," in *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, ed. Frederic Lemieux (London: Palgrave Macmillan, 2015), 51–61.

[47] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (January 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

[48] Clarke and Knake, *Cyber War: What It Is*, 157.

[49] Clarke and Knake, *Cyber War: What It Is*, 149.

Globalization Factor

Like nuclear war, cyberattacks ignore the barriers and borders in the real world. An attacker no longer needs to be near the scene or in reach of the defenders.[50] Net-speed collapses spatial distance to zero and allows actors outside a state's jurisdiction to exercise power against it with a good chance of never getting prosecuted.[51] This leads to a global cyber arena, where state actors are often bound by jurisdictions whereas their attackers evade their grasp easily.[52,53] Even more than in the nuclear age, such attacks can have a wide spectrum of effects that makes its scale hard to predict. A cyber tool like a virus can bounce back, spread to other countries, or create unpredictable global havoc in minutes.[54]

A further aspect of a globalized arena is the geopolitical symmetry, even for states not neighboring each other. If a state does not possess the escalation dominance (a favorable asymmetry of power and means), it might struggle to appropriately retaliate as it must fear to lose the escalations series in the end in the physical domain.[55]

Defense Factor

Unfortunately, the cyber realm lacks clear norms of what a proper defense and what an appropriate response are.[56,57] Besides the fact that cyber conflict skips the traditional battlefield and takes place in every-day systems (e.g., banks, television, and air traffic management,[58] the biggest challenge for deterrence is that offensive and defensive capabilities are kept under a code of silence. On the one hand, an opponent can prepare its own defense if he knows the adversary's offense and, on the other hand, there is no incentive to disclose a breach as it might ruin the reputation of the victim. Thus, there is no chance of learning from others and developing proper defense tools.[59] In the context of deterrence, this is counterproductive (as constant communication of clear and targeted deterrence decelerations is key) and must be overcome with a compromise of keeping

---

50 Goldsmith, "How Cyber Changes the Law of War," 53.

51 Betz, *Cyberspace and the State*, 39.

52 Clarke and Knake, *Cyber War: What It Is*, 30.

53 Andres, "The Emerging Structure of Strategic Cyber Offense," 92.

54 Goodman, "Cyber Deterrence," 116.

55 Estonia was reluctant to attribute the 2008 cyberattacks to Russia (even if it had good evidence) because of the geopolitical imbalance and the possible physical escalation of the far superior Russian military. See Goodman, "Cyber Deterrence," 109.

56 Carberry, "Why There's no Silver Bullet for Cyber Deterrence."

57 Andres, "The Emerging Structure of Strategic Cyber Offense," 101.

58 Clarke and Knake, *Cyber War: What It Is*, 30.

59 Andres, "The Emerging Structure of Strategic Cyber Offense," 93.

secret as much as possible but disclosing and communicating enough to effectively deter.[60]

Attribution Factor

Attribution was not a big issue in the nuclear age and, even today, with only nine states possessing nuclear weapons and well-known isotopic identifiers of each arsenal, it is a matter of minor concern.[61] But unlike nuclear weapons, cyber means are harder to trace back, and the hundred percent attribution to an originator is seldom possible.[62] The opinion is widespread that this thwarts the concept of deterrence, but in fact, even with an imperfect attribution, deterrence is possible, as long as three audiences are addressed[63]:

1. *The defending government* wants a relatively high assurance from its intelligence agencies and network forensics;
2. *The attacking government or non-state actor* knows what has been done but cannot be sure how good the opposing forensics and intelligence are; even if it denies the attack, it will never know how credible this deception was;
3. *The domestic and international public* needs to be convinced of the justice of retaliation. Therefore, a certain degree of detail needs to be disclosed, even if forensic methods can become useless for future cases.

The quality of attribution is a function of available resources, available time, and the adversary's sophistication. The less top-end forensic skills and highly experienced personnel are available, the lower the attribution quality will be. The higher the time pressure for attribution, the lower the quality will be. The more experienced and well-funded an opponent is, the lower the quality of attribution will be.[64]

Today it is less a question of *if* it is possible to attribute a cyberattack, but rather *how long* it will take.[65] As long as all cyberattacks follow the Cyber-Kill-Chain pattern[66] and involve a human adversary, there will be mistakes, individ-

---

[60] Goodman, "Cyber Deterrence," 109; Andres, "The Emerging Structure of Strategic Cyber Offense," 101.

[61] Nye, "Deterrence and Dissuasion in Cyberspace," 50.

[62] Clarke and Knake, *Cyber War: What It Is*, 68.

[63] Nye, "Deterrence and Dissuasion in Cyberspace," 51.

[64] Rid and Buchanan, "Attributing Cyber Attacks," 32.

[65] Tim Maurer, "Here's How Hostile States Are Hiding behind 'independent' Hackers," *The Washington Post*, February 1, 2018, www.washingtonpost.com/news/monkey-cage/wp/2018/02/01/heres-how-hostile-states-are-hiding-behind-independent-hackers.

[66] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1, no. 1 (2011):

ual motivations, and relationships that make the tracing, fighting and deterring possible.[67] This fact brings up another parallel to the nuclear age. Dealing with humans cannot be done virtually or from behind a computer. The best way to attribute an attack after it happened is to already have an intelligence campaign of infiltration and trusted contacts in place.[68] This rather traditional HUMINT intelligence techniques become important again and may outpace the recently preferred and convenient signal intelligence (SIGINT).[69]

Legal Framework of Cyber Space

Like the advent of nuclear weapons, the information age brought game-changing modern technologies that altered the way IR and their legal frame were to be seen. Some even argue that these new technologies outpaced law and that recent legislation cannot fully govern emerging cyber capabilities.[70,71] But as isolated solutions of single actors cannot work, only International Law (IL) is able to provide a legal framework. It still tries to grasp the implications of a digitized world and needs time to translate it into a cyber-specific treaty and customary law. Until then, cyberspace's escalation potential stays significant, as states can rely on leeway by resorting to differing interpretive positions.[72] The only way to reduce this destructive potential is to provide a stable and accepted legal framework.

In 2013, the UN's Group of Governmental Experts agreed that International Law—and in particular the Charter of the UN—is applicable in the cyber do-

1–14, 5, www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

67 "Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model," Complimentary Report (Milpitas: FireEye Inc., June 2014), www.iqpc.com/media/1003877/33776.pdf.

68 Carr, "Responsible Attribution," 8.

69 Clarke and Knake, *Cyber War: What It Is*, 215.

70 This reaches relevance in the context of the "Presumptive Legality" of International Law, which says that acts that are not forbidden are permitted. As modern information technologies are not explicitly considered in International Law, there is a lot of leeway for states as long as the gaps are not closed by custom law or explicit treaties. See Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York, NY: Cambridge University Press, 2016), 51, Rule 11.9.

71 Michael N. Schmitt, "The Law of Cyber Targeting," Tallinn Paper No. 7 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/uploads/2018/10/TP_07_2015.pdf.

72 Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," Tallinn Paper No. 5, Special Expanded Issue (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014), https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf.

main.[73] This groundbreaking position by an internationally recognized body was the first crucial step to fill the legislative vacuum in cyberspace. It was accompanied by the release of the "Tallinn Manual on the International Law Applicable to Cyber Warfare" and followed by the Tallinn Manual 2.0 in 2017, which were drafted as non-binding studies under the leadership of the NATO CCDCOE.[74] The EU even went beyond that opinion by stating in its Cyber Security Strategy that "the same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain."[75]

Accordingly, for all states, the rules of engagement in the cyber arena are defined by IL's conditions, and to find an effective and credible deterrence position, the following points need clarification:

- How to classify a cyberattack under international law?
- What kind of response to a cyberattack is lawful?
- Which targets are lawful in a cyber-exchange?

Classification of a Cyber-Attack under International Law

The Tallinn Manual 2.0 states that "the principle of state sovereignty applies in cyberspace," and thus, a state can take all measures not prohibited by IL that it considers necessary and appropriate to deal with its cyber infrastructure, with actors in the cyber domain or with cyber activities within its territory.[76,77] Consequently, every hostile cyber operation aimed against a state's cyber and non-cyber infrastructure means a violation of sovereignty if physical harm or injury is caused.[78] This is not the case if an attack manipulates or deletes databases to cripple the economy or to influence political processes. Although several schol-

[73] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (United Nations General Assembly, 2015), 12, https://digitallibrary.un.org/record/799853.

[74] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/.

[75] Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace (Brussels: European Union, 2013), 3, https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en.

[76] Michael N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York: NATO Cooperative Cyber Defence Centre of Excellence, 2017), 11.

[77] Cited in Jasper, *Strategic Cyber Deterrence*, 142.

[78] Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law*, 54, (2014): 697-732.

ars demand to include these non-physical effects, they are still out of scope in the common interpretation.[79]

Cyber operations are non-kinetic in nature, and therefore often misperceived as non-forceful, although their effects can range from simple annoyance to death. Thus, cyberattacks need to be assessed according to their effects on the real world, and if they have an outcome comparable to a kinetic attack, they constitute a "use of force."[80,81] However, a state is only allowed to conduct forceful defensive actions in the case of an "armed attack," which means the use of force must reach a certain threshold.[82,83] This edge sometimes is kept in a strategic ambiguity to make the prediction of potential self-defense actions harder for the adversary.[84] The Tallinn Manual 2.0 becomes concrete only for acts of cyber intelligence gathering, cyber theft, and brief interruption of non-essential services, which do not qualify as armed attacks due to the lack of serious injuries or deaths or the cause of severe damage.[85,86] For attacks that do not reach the threshold of an armed attack but that are an unlawful use of force, only countermeasures aimed to stop the attack are utilizable.[87] If the use of force mounts

---

79 Michael N. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," *Villanova Law Review* 56, no. 3 (2011): 569-605, 574; Schmitt and Vihul, "The Nature of International Law Cyber Norms," 17.

80 The UN Charter prohibits the use or threat of force by demanding: "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." See United Nations, "Charter of the United Nations" (United Nations, 2016), Article 2 (4).

81 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 573.

82 This can also be the case, if a series of cyber incidents (that individually would fall below the threshold of an armed attack) aggregate. Therefore, they must have the same originator, must be related, and taken together must have the requisite scale. see Schmitt, *Tallinn Manual on the International Law*, 56, Rule 13.8.

83 United Nations, "Charter of the United Nations," Article 51.

84 In line with that, the 2014 NATO Summit in Wales decided to determine if a cyberattack would lead to the invocation of article 5 (and thus, be considered as armed attack) on a case-by-case basis. See Schmitt and Vihul, "The Nature of International Law Cyber Norms," 26. In the opinion of Lewis, "Rethinking Deterrence," 9, this strategic ambiguity of thresholds creates confusion and dilutes the deterrence effects. The NATO nuclear strategy of "Flexible Response" in contrast, held its escalation ladder in a strategic ambiguity (aware that the capabilities were known anyway) but made the redlines very clear. See Kenyon and Simpson, *Deterrence and the New Global Security Environment*.

85 Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law*, 339.

86 Cited in Jasper, *Strategic Cyber Deterrence*, 142.

87 The Tallinn Manual 2.0 states in rule 20 that states are entitled to take countermeasures (cyber or non-cyber) in response to the breach of international legal obligation by another state. Rule 69 says that cyber operation constitutes a use of force if they

to an armed attack, carried out through the instrument of classic military force causing or risking destruction of property and injury or death, then forceful defensive action is permitted. Should the cyber operation be a component of an overall military action, it constitutes an armed attack, even if it independently would not qualify as such.[88] Consequently, states have an incentive to quickly treat pure cyber operations as an armed attack to justify a forceful defensive response, increasing the likelihood of escalation significantly.[89]

Lawful Responses to a Cyber-Attack

A state that falls victim to an unlawful cyber operation has certain rights under international law if the attack reaches at least the level of the use of force. This starts with the always lawful claim for compensations for physical or financial losses and non-forceful responsive actions like blocking incoming data transmissions. Above that, typical technical, political, or economic countermeasures aiming at cessation and reparation can be taken in response to an identified use of force. These measures can involve a limited degree of military force and would normally be contrary to international obligations, but are lawful if proportionate to the injury suffered and below the threshold of an armed attack. However, the opposing state needs to be called in advance to refrain from going on or to take measures to stop acts emanating from its territory.[90,91] The right to take countermeasures is reserved for states, even if there are private IT-companies with cyber capabilities that exceed the state's arsenal. Nevertheless, the Tallinn Manual 2.0 explicitly mentions the right of an injured state to turn to private firms to conduct cyber operations on its behalf. Of course, the responsibility for the countermeasures conducted by the privateer stays with the state.[92,93]

If the use of force mounts to the level of an armed attack (no matter if initiated by a state or a non-state actor), the right of self-defense applies, and necessary and proportionate forceful actions can be conducted against an attacking

---

have comparable effects like non-cyber operations that would qualify as use of force. Countermeasures in this case can only be aimed to remedy existing harm as long as the threat exists and not for retaliation purposes. Furthermore, the adversary has to be warned in advance to give him the chance to cease the attack. See Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law*, cited in Jasper, *Strategic Cyber Deterrence*, 174.

88 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 587.

89 The US approach in this matter bears exactly this danger but seems to be effective in the cyber arena, as all uses of force are considered as armed attack and may be answered forcefully. See Schmitt, "'Below the Threshold' Cyber Operations," 730.

90 Schmitt, *Tallinn Manual on the International Law*, 36, Rule 9.

91 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 581.

92 Schmitt, "'Below the Threshold' Cyber Operations," 727.

93 Jasper, *Strategic Cyber Deterrence*, 179.

opponent.[94] As there is no international consensus on the borderline between the use of force and armed attack, this becomes a matter of interpretation and persuasive power of the injured state, as IL does not dictate the level of certainty of attribution to act in self-defense.[95] The question arises, how to respond to non-state actors, which, per definition, cannot violate the prohibition of the use of force under the international law made for states. In such cases, state responsibility offers an option to apply IL anyway. A state is not only responsible for the actions of its governmental organs but also for the conduct of individuals or groups that act on the instructions or under the control of the state.[96] Furthermore, a state can be held responsible for unlawful acts of non-state actors in its territory if it fails to take appropriate measures to stop the attack or provide all available support to investigate the incident.[97,98] If this state is unwilling or incapable to fulfill its legal duty, the victim state can act in self-defense and stop the attack with kinetic or cyber means, even on the other state's territory. But self-defense is not only possible in response of an ongoing armed attack. It can also be conducted facing an imminent attack (evidenced by hostile actions like preparatory cyber operations that will result in effects on the armed attack level) with no other reasonable hope of fending it off than responding immediately.[99]

Lawful Targets in a Cyber-Exchange

If the situation mounts to the point where forceful self-defense or retaliation becomes a lawful option, the question of how and what to attack arises. The cyber domain is characterized by pervasive dual-use infrastructure, which might be designated for civilian use but can by nature, location, purpose, or use be utilized for military purposes.[100] Thus, this infrastructure becomes a lawful military target under International Humanitarian Law (IHL), as the total or partial destruction, capture, or neutralization offers a direct and concrete military advantage. Ultimately this means that due to the heavy reliance on civilian products and infrastructure, the range of targetable objects in the cyber arena ex-

---

94 Schmitt, *Tallinn Manual on the International Law*, 54, Rule 13.

95 Carr, "Responsible Attribution," 7.

96 The International Court of Justice (ICJ) provided the precedence with the ruling on the Nicaragua case, in which it held the US responsible for breaches of International Humanitarian Law committed by a rebel group the US "effectively controlled." See Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 578.

97 The ICJ provided the precedence in the Corfu Channel case with the decision that a state violates its international obligations if it allows knowingly its territory to be used for unlawful acts against other states. See Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 578.

98 Goodman, "Cyber Deterrence," 108.

99 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 592.

100 This can be airspace management systems or communication lines that are partly used for military intentions.

pands, and systems with important civilian functions can legally be affected.[101] In the case of a forceful response in a cyber exchange, this brings certain flexibility in choosing targets but, at the same time, cyber means face the issue of difficult scalability and specific targeting. IHL requires that a weapon discriminates between combatants and civilians or civilian and military objects. If a cyber weapon cannot be directed at a specific military objective or generates uncontrollable effects, its employment is prohibited.[102] These restrictions do not apply for defensive measures and non-forceful means like malware that does not cause injury, damage, or loss of system functionality, even if it can spread into civilian systems.[103] If non-combatants that are not affiliated with an organized armed group and not under the control of a state are involved in a cyberattack, they can be targeted for the time they take direct part in the hostilities. In the cyber arena, this can start with gathering and spreading military intelligence by cyber means, probing an adversary's systems to identify vulnerabilities, or developing software specific to an attack.[104]

Application of Deterrence in the Cyber Domain

By considering the experiences made with the basic mechanisms of deterrence and by respecting the special implications and the legal characteristics of the cyber domain, it becomes clear that cyber deterrence cannot be applied in isolation but must be one vital component of a comprehensive security strategy.[105,106] In contrast to the nuclear concepts, defenses and resilience are a fundamental starting point to deny an adversary's success.[107] Besides *denial* by defense, the classical deterrence aspect of *retaliation* as threat of punishment plays a major role. As this research is based on a broader understanding of deterrence, two more ways come into focus: Deterrence by *entanglement* and by establishing *normative taboos*.[108]

Deterrence by Denial

Focusing on the defensive side becomes more important as the number of potential state adversaries with offensive cyber capabilities is on a steady rise.[109]

[101] Schmitt, "The Law of Cyber Targeting," 11.

[102] Inspite of this, if a cyber weapon is an alternative to a kinetic one and has a similar effect on the opponent, it ought to be preferred, as in most cases collateral damage is less likely, see Schmitt, "The Law of Cyber Targeting," 18.

[103] Schmitt, "The Law of Cyber Targeting," 16.

[104] Schmitt, "The Law of Cyber Targeting," 14.

[105] Nye, "Deterrence and Dissuasion in Cyberspace," 46.

[106] Cooper, "A New Framework for Cyber Deterrence," 105.

[107] Carberry, "Why There's no Silver Bullet for Cyber Deterrence."

[108] Nye, "Deterrence and Dissuasion in Cyberspace," 54.

[109] The Worldwide Threat Assessment of the US Intelligence Community shows a rise

Deterrence by denial aims to build resilience and the capacity to recover. Thereby, the adversary's benefits of an attack can be reduced until an engagement becomes futile and, after a blow, it can be ensured that cyber and non-cyber military responses are accessible for retaliation. There are measures of different sophistication and costs available,[110] but all have the common goal of chewing up the attacker's resources and time and disrupting his calculus of the perceived gain probability and value.[111,112] According to the "Assumed-Breach-Paradigm" there is no way of eliminating the successful penetration of one's networks. But the breech can be crafted difficult and tedious. Consequently, an attacker makes more "noise," needs more time, and becomes easier to identify as he leaves more traces.

On the way to a resilient culture, private-public-partnerships (PPP) and cyber insurances play a vital role. PPPs, on the one hand, bring together the government (as a legislator with rich resources in manpower, which is not focused on profit but effectiveness and can rely on intelligence services) with efficiency-driven privateers (who are highly experienced and technically specialized in the cyber domain, where they can access a large quantity of data and information).[113] On the other hand, mandatory cyber insurances for the economy contribute to systemic resilience and the denial of holding a nation's economy at risk. By putting a price tag on various private cyber practices, an incentive for higher standards and minding a "basic cyber hygiene" arises, whereby the low hanging fruits can be taken off the table and quick wins can be attained.[114] Furthermore, the reporting and connecting of attack-related data could be boosted significantly by profiting from the insuring industry's sophisticated crisis reaction

---

from probably three states in 2007 to over 30 states in 2017. See Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community" (Washington D.C.: Director of National Intelligence, February 2018), 6, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[110] An example for sophisticated and expensive measures is stockpiling redundant industrial power generators and transformers. Example for easy and cheap measures: Military training in celestial navigation in case of loss of global positioning systems. See Nye, "Deterrence and Dissuasion in Cyberspace," 56.

[111] Nye, "Deterrence and Dissuasion in Cyberspace," 56.

[112] Jasper, *Strategic Cyber Deterrence*, 111.

[113] The US government emphasizes this approach in its National Security Strategy: "In accordance with the protection of civil liberties and privacy, the U.S. Government will expand collaboration with the private sector so that we can better detect and attribute attacks." See *National Security Strategy of the United States of America* (Washington D.C.: The White House, 2017), 13, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[114] With relevant training to increase user awareness, up to 50 % of incidents could be avoided. See "ENISA Threat Landscape Report 2016" (Heraklion: European Union Agency for Network and Information Security, 2017), 81, www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport.

centers and processes.[115] Thus, the information asymmetry between privateers and government can finally be reduced, the reaction times can be increased, and the ground for a trust-based information sharing culture can be provided. To additionally foster private-public cooperation, "responsible disclosure agreements"[116] and "temporary clearances"[117] should be implemented.

Further starting points to improve the resilience and recovering capabilities can be found in the structure of the defense itself. It cannot be enough to protect only the outer perimeters of a system. As a breach is possible at any time, there are measures for an in-depth defense, able to detect the attacker inside the system, trace, identify, and disturb him. This can be supported by segmented networks and segmented sectors that do not allow, once a perpetrator is in, to spread his access over the entire system. Keeping vital capabilities as redundancies might be expensive at first glance but significantly lowers the gain probability of the adversary. Finally, protecting the supply chain is indispensable to avoid an opponent sneaking in. This requires an intense security-by-design debate with a consequent vetting of manufacturers and service providers and assessment which parts of critical supply chains need to be under national control.

Deterrence by denial is more than the mere repelling of a cyberattack. Conducted in a comprehensive manner, it can increase the time and survival factor, relive the force factor and provide the basis for the attribution factor on which retaliation becomes possible. If communicated in an appropriate way, the defense capabilities of a state can significantly influence the opponent's calculus of gain value and gain probability and give the government the leeway to pivot to major threats in the cyber arena.[118]

Deterrence by Retaliation

Responding to unwanted behavior with punishment is the most prominent way of deterrence. The goal is to promise to inflict costs on the attacker that outweigh the benefits anticipated from the initial attack.[119] This only works if the

[115] Umar Choudhry, *Der Cyber-Versicherungsmarkt in Deutschland: Eine Einführung* (Wiesbaden: Springer, 2014).

[116] Agreement between finder of vulnerabilities and software manufacturer to meet a publication deadline. The finder avoids the risk of being hold responsible for the exploitation of a vulnerability, the manufacturer receives appropriate time to analyze and fix the vulnerability and the user can rely on the fact that patches are not prolonged more than necessary. See *Die Lage der IT-Sicherheit in Deutschland 2017* (Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2017), 21, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf.

[117] Temporally limited, case-related suspension of security clearances for a task-force to enable efficient information sharing amongst agencies and involved privateers.

[118] Nye, "Deterrence and Dissuasion in Cyberspace," 56.

[119] The US will "…impose swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities." See

attack can be attributed to an adversary in a sufficient way, addressing the three above-mentioned audiences.[120] Retaliation does not have to stay in the cyber domain but can take the shape of diplomatic, informational, military, and economic actions tailored to the opponent and considering potential back coupling effects due to international interdependencies.[121] Besides, geopolitical symmetry plays a key role. Retaliating against an adversary can mean to actuate an escalating series of retaliations outside the cyber arena, which in the long run can only be won if the escalation dominance lies on one's side.[122]

Countermeasures inside the cyber realm can be manifold and contain various levels of aggressiveness.[123] Outside the cyber domain, sanctions are the most common response to unwanted behavior, though in most cases they affect the population of a state more than the government. Therefore, it turns out to be more effective to invest resources in identifying attackers and aim sanctions on those individuals.[124] Even if no specific individual can be named, it is still possible to aim retaliation measures on relationships and social networks in which the attackers participate. This works, as all attackers are bound by dependencies and their calculus of gain and loss can be affected indirectly. Suspected groups can be cut from privileges like participating in the financial community and public outrage can be used to put internal pressure on the perpetrators and even outlaw them to the point where the network turns against them to avoid harm.[125]

Effective retaliation needs the time, force, survival, and attribution as baseline to contribute to the defense factor. Kinetic means have proved to be efficient tools of statecraft to respond to cyberattacks. As a result, conventional military means can be chosen as well as a nuclear answer in extremely severe cases.[126]

National Security Strategy of the United States of America, 13; Goodman, "Cyber Deterrence," 106.

[120] Nye, "Deterrence and Dissuasion in Cyberspace," 51.

[121] Jasper, *Strategic Cyber Deterrence*, 13.

[122] Goodman, "Cyber Deterrence," 109.

[123] As proposed in ascending order in Jasper, *Strategic Cyber Deterrence*, 177:
- Allow attackers to steal bogus files or embed beacons that reveal their location
- Bait files with malware to photograph the malicious actors using their webcam
- Infiltrate malicious actor networks to retrieve, alter or delete stolen data
- Implant malware to damage or ransomware to lock down actor computers
- Insert logic bombs into files before stolen to damage computers when opened
- Use DDoS attacks to interfere with malicious activity.

[124] President Obama did exactly this, by signing an Executive Order to block property and interests of people found to be meddling with the IT systems of the US's critical infrastructure. See Jasper, *Strategic Cyber Deterrence*, 97.

[125] Cooper, "A New Framework for Cyber Deterrence," 114.

[126] In the newly drafted nuclear strategy of the U.S., the possibility of nuclear retaliation for devastating cyberattacks is explicitly envisaged. See David E. Sanger and William J.

Deterrence by Entanglement

The modern international system is characterized by various dependencies, interconnections, and shared vulnerabilities. Deterrence by entanglement tries to encourage responsible state behavior by emphasizing the return from cooperation on mutual interests.[127] If an attack has negative back coupling effects on the attacker and benefits the status quo and its continuation, malicious engagement loses attractiveness. Entanglement boosts the survival and globalization factors and increases the adversary's perception of loss value and probability, even if the attack is not actively defended against or there is no fear of retaliation. The deterrence effect is contingent on a complex international deterrent relationship and works better when interdependencies are stronger.[128]

To enhance the effects of entanglement, confidence-building measures are an appropriate tool to strengthen international peace and security by increasing interstate cooperation, transparency, predictability, and stability.[129] In the cyber arena, communication hotlines, regional communication centers, prenotification agreements, and agreements on not attacking specific targets are feasible options and can be supplemented by forensic assistance in an IT incident and noninterference agreements with the workings of computer emergency response teams. Only establishing a cyber arms control regime faces some difficulties. Most technologies that could be described as cyber weapons are dual-use (like vulnerability assessment programs that can either find security gaps to protect a system or to exploit it) and, as a result, there is no consensus on what a cyber-weapon really is.[130] Above that, verifying the stock of cyber arms is nearly impossible, as this weaponry is not tangible and can easily be hidden or recreated after deletion.[131] To tackle this issue, "effects" instead of "used weapons" must be addressed.[132] In addition, normative taboos can be established, which is the last of the four ways of cyber deterrence.

Deterrence by Normative Taboos

With established strong norms, an aggressive actor will suffer reputational costs that will damage its soft power beyond the value gained from the attack. If a

---

Broad, "Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms," *The New York Times*, January 16, 2018, www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html.

[127] Jasper, *Strategic Cyber Deterrence*, 16.

[128] China, which takes the legitimacy of its ruling party out of economic growth and thus depends on the internet, is far more entangled with the western world than the rather isolated North Korea. See Nye, "Deterrence and Dissuasion in Cyberspace," 58.

[129] Jasper, *Strategic Cyber Deterrence*, 150.

[130] Jasper, *Strategic Cyber Deterrence*, 16.

[131] Nye, "Deterrence and Dissuasion in Cyberspace," 60.

[132] Goodman, "Cyber Deterrence," 116.

state breaks a taboo (e.g., using nuclear weapons in a minor conflict against a weaker state), it faces the danger of being ostracized by the international system. This deterrence effect works although there is no active defense or a credible retaliation, but needs a certain degree of attribution. In history, the international community agreed on several implicit and explicit norms, such as the prohibition of chemical and biological weapons in the Geneva Convention.[133]

In the cyber domain, the normative agreement on the applicability of international law and the United Nations Charter was the first important step. In 2013, the UN's "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" proposed basic norms, like meeting the international obligations if a wrongful act gets attributed to a state, not to use proxies and not to tolerate non-state actors using a state's territory to commit wrongful acts.[134] Also, the use of International Tribunals and the International Criminal Court for the conviction of cybercriminals, terrorists, and state actors can be a powerful norm to deter and transmit a warning message.[135] Cyber-related norms can guide state behavior and increase predictability, trust, and stability in cyberspace as well as reduce the potential for conflict due to misperceptions. This only works, if norms are accepted by the majority of states and become institutionalized over time, e.g., under the umbrella of the UN.[136] Normative taboos can contribute to a certain extent to control over cyber weapons, even if it is impossible to establish a cyber arms control regime. They need to focus on tabooed effects and targets and, thus, can help distinguish which behavior is tolerated and which is ostracized.[137]

Conclusion

It became apparent that basic mechanisms of deterrence work in all realms, also in the cyber domain. Especially, as nuclear deterrence loses relevance in IR and current conflicts are ever more characterized by cyber components, the need for a comprehensive understanding of cyber deterrence is undeniable. Moreover, it was shown that five underlying factors (time, forces, survival, globalization, defense) of a game-changing new technology like the atomic bomb can be adapted to the cyber age. Above that, attribution plays a crucial role in the cyber domain and needs to be added to the discussion. It became clear that the international system is still in an early stage of applying IL in the cyber domain and that legislation must go a long way to catch up with the technological developments.

---

[133] Although this taboo did not stop Bashar al-Assad from using chemical weapons against his population, the international reaction (dismantling of Syrian chemical weapons in 2014 and the US led retaliation attacks of 2018) reflected the increased costs for breaking a normative taboo. See Nye, "Deterrence and Dissuasion in Cyberspace," 60.

[134] Jasper, *Strategic Cyber Deterrence*, 17.

[135] Quinlan, "Deterrence and Deterrability," 8.

[136] Jasper, *Strategic Cyber Deterrence*, 145.

[137] Nye, "Deterrence and Dissuasion in Cyberspace," 60.

The derived four ways to apply deterrence in the cyber domain (denial, retaliation, entanglement, and normative taboos) provide a feasible approach to integrating cyber deterrence aspects into a state's cybersecurity strategy (knowing that cyber deterrence can be only one pillar of an overall security strategy). However, those ways never work in an isolated way but rather in a comprehensive package with variable weighting of the single elements.[138] By complying with the basic mechanisms of deterrence and by tailoring the package to specific threat actors, a versatile and sound deterrence becomes possible.

Therefore, the hypothesis of this work can be validated: *Even in the cyber age, deterrence can be a powerful tool of statecraft and contribute to the protection of a state's national security interests!*

Still, effective deterrence does not arise by itself. It needs to be managed strategically or its effects will not be controllable. Politicians and strategists all around the world must prepare for a new and demanding age of deterrence to avoid sleepwalking into a real cyberwar.

In a subsequent article, the present findings will be applied in the example of Germany. It will be explained how Germany as an important player in an ever more digitized international system, can approach a cyber deterrence strategy to bolster its national security interests.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Manuel Fischer is a security professional, working in the German defense sector with focus on counter-UAS Solutions. He looks back on twelve years of service in the German military (Bundeswehr) as a military police officer. During this time he acquired a Master of Science in Economics and Organizational Science from the University of the Federal Armed Forces in Munich. His service in the military was followed by his studies at the George C. Marshall European Center for Security Studies where he graduated its Master's program of International Security Studies concentrating on cyber security.
E-mail: fischermanuel@web.de.

[138] E.g., against the rather isolated North Korea, entanglement cannot be a major part of the set of the strategy, whereas against the powerful Russia, entanglement plays a far bigger role than retaliation.

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

T. Maliarchuk, Yu. Danyk, Ch. Briggs
Connections QJ 18, no. 1-2 (2019): 93-110
https://doi.org/10.11610/Connections.18.1-2.06

Research Article

Hybrid Warfare and Cyber Effects in Energy Infrastructure

***Tamara Maliarchuk,*[1] *Yuriy Danyk,*[2] *and Chad Briggs*[3]**

1 *Zhytomyr Ivan Franko State University, https://zu.edu.ua/en_index.html*

2 *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," https://kpi.ua/en*

3 *University of Alaska, Anchorage, USA, https://www.uaa.alaska.edu/*

Abstract: Energy is an integral part of all branches of the economy and social sphere, with a special role in ensuring the security of the development of modern society. Therefore, energy infrastructure has become a critical component of the hybrid war. Destructive cyber bullying in it is accompanied, as a rule, by chain effects and synergistic effects that systematically influence and cover all other spheres of the life of society and the state, both in ordinary and, especially, in critical conditions. The authors systematically and comprehensively analyzed and present in this article the results of investigations of the features of destructive cyber defects in the national energy sector of Ukraine and the ways of counteracting and protecting critical energy infrastructure.

Keywords: hybrid warfare, power complex, energy infrastructure, cybersecurity, cyberattack.

Introduction

Discussions of hybrid warfare have often centered on definitional debates over the precise nature of the term, and whether 'hybrid' covers what other military experts describe as nonlinear warfare, full-spectrum warfare, fourth-generation warfare, or other such terms. Similarly, discussions of cyber conflict have treated the phenomenon as a separate domain, as if using cyber tools remained distinct

Creative Commons BY-NC-SA 4.0

from other forms of conflict. A hybrid war that is *de jure* being conducted on the territory of Ukraine, and *de facto* encompassing more participants all over the world in terms of its content, forms, and methods of conducting, can be considered a specific variant of fourth-generation wars (4GW).

In hybrid conflicts of any intensity, hostilities (operations) are an element of other (non-force) actions mutually coordinated according to a single plan, mainly economic, political, diplomatic, informational, psychological, cyber, cognitive, among others.[1] This creates destabilizing internal and external processes in the state that is the object of aggression such as concern and discontent in the population, migration, and acts of civil disobedience. Hybrid wars are not declared and, therefore, cannot be completed in the classical sense of the end of wars and military conflicts. This is a kind of permanent war of variable intensity across multiple sectors, with cascading impacts and synergistic destructive manifestations, in which the entire population of the country and the international community are, to a certain extent, consciously or unconsciously involved. The impacts are felt on all spheres of life, on all sectors of society, and throughout the state. Thanks to the use of innovative technologies, it became possible to shift conflict from predominantly overt and forceful (kinetic) means to less obvious strategies focused on the structural vulnerabilities of adversaries, including (importantly) achieving cognitive advantage over them.

When applied to events in Ukraine since 2013, the primary focus has often been on the Russian invasion of Crimea in 2014, and the subsequent support of Russian backed enclaves in the eastern Ukrainian regions of Donbass and Lugansk. These operations, from the appearance of so-called "little green men" in Simferopol to the downing of Malaysian Airlines flight 17 several months later, focus on fairly conventional (if irregular) forms of conflict. What is often missed are the broader strategic goals of an adversary in undertaking a hybrid war campaign and the broad spectrum of tools used to achieve those goals.

As many authors have argued, hybrid warfare is not a new phenomenon, as it represents coordinated actions by both state and non-state actors to conduct a campaign of actions that span from information warfare to direct, kinetic conflict.[2] The strategies of the Russian Federation toward post-Maidan Ukraine have centered largely on the goals of destabilizing and delegitimizing the government, part of an effort to prevent Ukrainian integration with Western European institutions and to prevent effective intervention by Western or NATO countries.[3]

---

1 Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, "Hybrid War: High-tech, Information and Cyber Conflicts," *Connections: The Quarterly Journal* 16, no. 2 (2017): 5-24, https://doi.org/10.11610/Connections.16.2.01.

2 Robert Wilkie, "Hybrid Warfare: Something Old, Not Something New," *Air and Space Power Journal* 23, no. 4 (Winter 2009): 13-18; NicuPopescu, "Hybrid Tactics: Neither New Nor Only Russian," *EUISS Issue Alert* 4 (European Union Institute for Security Studies, January 2015), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf.

3 Emmanuel Karagiannis, "The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy and Goals," *Contemporary Security*

While the occupation of Crimea and the continued conflict in eastern Ukraine help to serve this purpose, a larger but less visible array of actions have been undertaken to target the resilience of Ukrainian institutions. Rather than focus on the hybrid war itself, or cyber as a separate domain, the purpose of this article is to illustrate and explain the use of cyber weapons against the energy infrastructure.

Again, while not a new strategy, whether by insurgents or strategic bombing campaigns, the targeting of energy infrastructure is an effective way to increase the vulnerability of a state or society while signaling to other potential adversaries their own vulnerabilities and the potential to cripple large sectors of the economy. Cyber tools provide an asymmetric advantage without regard to geographic distance, meaning that small groups can inflict widespread damage while avoiding normal attribution and the rules of deterrence.[4] During the Cold War, the United States conducted hybrid operations in countries such as the Philippines in the early 1950s and Vietnam in the 1960s, using an array of techniques from establishing newspapers and radio stations, to supporting insurgents and mercenaries, to the active involvement of US combat troops. The US experience may be instructive, in that it provides illustrations of two very different strategic goals in employing hybrid techniques – of either trying to stabilize or destabilize a foreign regime. While, in some cases, such as the Philippines, stabilization efforts were largely successful, in examples from Vietnam to Afghanistan, the US has had far less success in its stabilization efforts. Destabilization, on the other hand, appears to be a more commonly successful use of hybrid warfare techniques as, for example, in the controlled US actions in Central America and Chile, or in Iran in 1953.[5]

For purposes of this and subsequent articles, hybrid warfare is defined as the full-spectrum use of state and non-state instruments to shift the stability and legitimacy of key systems and institutions in a given region. Note that this, theoretically, means that hybrid warfare methods can be used to legitimate purposes as well as to destabilize, and this is often done when attacking an adversary while concurrently promoting support of one's own state and allies/ proxies. While the dual use of hybrid tools is not as obvious in the energy sector, this article is one of a series that also examines social resilience and the role of foreign intervention (e.g., the European Union's relations with Ukraine) where playing multiple

Policy 35, no. 3 (2014): 400-420, https://www.tandfonline.com/doi/abs/10.1080/13523260.2014.963965; Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare" (Washington: Institute for the Study of War, 2015), http://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

4 Dinos Kerigan-Kyrou, "Critical Energy Infrastructure: Operators, NATO, and Facing Future Challenges," *Connections: The Quarterly Jpurnal* 12, no. 3 (Summer 2013): 109–17, http://dx.doi.org/10.11610/Connections.12.3.06.

5 Max Boot, *The Road Not Taken: Edward Lansdale and the American Tragedy in Vietnam* (New York: Liveright Publishing, 2018).

roles becomes more important, and where cyber techniques make these efforts ever more difficult to track. Energy infrastructure and cyberattacks are a useful place to start because of the existing history of attacks, and the similarities shared between states in their need to protect energy supplies and their vulnerabilities to cyber tools.

These are not capabilities limited to Russia. The Stuxnet worm (possibly attributed to Israel and the US) was effective in inflicting physical damage on nuclear fuel centrifuges not connected to any outside network and regarded by the Iranians as safe from outside interference or attack. Stuxnet was an elegant piece of programming that could easily move from computer to computer without detection, not harming or interfering in any system until it finally found its way to specific computer-controlled centrifuges in Iran. Once there, the worm would make slight changes to the operation of the high-speed machines, shifting the calibration just enough to damage or destroy them, without raising suspicion that an outside attack was occurring.[6] Likewise, China and even smaller powers such as North Korea possess anti-energy cyber capabilities, and non-state actors such as Al Qaeda and ISIS have also exhibited notable cyberattack capabilities against energy.[7]

The Concept of Resilience

As Conklin and Kohnke wrote, much of cybersecurity has been built around the concept of 'walling off' computer systems to outside intruders and protecting data rather than focusing on the resilience of the system as a whole. Their argument was to focus more on functionality rather than on individual attacks, a focus that already exists in the energy sector but indicates a mismatch between energy security and the vulnerabilities present in infrastructure from cyber-related systems.[8] Energy security from cyberattacks, therefore, relies on a broader concept of resilience, one tied not only to actual production and transmission of energy but to those systems that energy supports and legitimates. If energy is removed from a society, particularly a highly industrialized and technology-dependent one, then the proverbial rug is being pulled out from under all support systems.

Resilience networks can be modeled according to the type and pattern of

---

6 Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy* 9, no. 3 (May-June 2011): 49-51.

7 Lukáš Tichý and Jan Eichler, "Terrorist Attacks on the Energy Sector: The Case of Al Qaeda and the Islamic State," *Studies in Conflict & Terrorism*, 41:6 (2018): 450-473, https://doi.org/10.1080/1057610X.2017.1323469.

8 William Arthur Conklin and Anne Kohnke, "Cyber Resilience: An Essential New Paradigm for Ensuring National Survival," in *Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018*, National Defence University, Washington D.C., USA, 8-9 March 2018, ed. Dr. John S. Hurley and Dr. Jim Q. Chen (Reading, UK: Academic Conferences and Publishing International Limited, 2018), p. 126.

connections (topology) between different parts of the system, whether these are individuals, electrical connections, or ecological relationships. Since network connections are functional, they are rarely random, and instead, center on critical nodes that provide crucial links within the system. In ecological sciences, these critical nodes are often referred to as "keystone species" which, even if they are not the most visible representatives of an ecosystem, are crucial to its effective functioning. In social systems, these critical nodes may be key individuals or centers of community activity, which provide a focus in connection between people who otherwise may not interact. And with the Internet, critical nodes are either the more visible centers of activity such as Google, or can be represented in terms of key servers or communication lines. In all of the above cases, however, these networks are often known as "scale-free," meaning they tend to be resilient because random failures at any part in the system can be compensated for.[9]

Energy networks are often configured differently, as, instead of being resilient and allowing for re-routing of power in the case of failure, traditional energy infrastructure has been constructed on centralized nodes. The pattern of energy infrastructure from the twentieth century was one of large power plants (either fossil or nuclear fueled) which then transmit electricity to population centers, with corresponding subnetworks of electrical transformers.[10] Much of the work on increasing the resilience of energy systems has focused on preventing cascading failures in electrical networks, where the failure of a few critical nodes propagates blackouts over large geographic areas, as witnessed numerous times in North America. This was a form of resilience, but one coupled with aspects of fragility, meaning the system was brittle and could easily be broken with enough external force. The experience of Puerto Rico in the wake of Hurricane Maria in 2017 has been an unfortunate case in point.[11] Civilian resilience for the energy sector focuses less on the power plants themselves, although, increasingly, environmental factors have overwhelmed the ability of large power plants to withstand flooding and other environmental hazards. While the Fukushima disaster in 2011 was the most visible example, increasingly energy utilities in North America and Europe have become more vulnerable.[12]

---

[9] Sarah Dunn and Sean Wilkinson, "Hazard Tolerance of Spatially Distributed Complex Networks," *Reliability Engineering & System Safety* 157 (2017): 1-12.

[10] Dong Hwan Kim, Daniel A. Eisenberg, Yeong Han Chun, and Jeryang Park, "Network Topology and Resilience Analysis of South Korean Power Grid," *Physica A: Statistical Mechanics and Its Applications* 465 (January 2017): 13-24, https://doi.org/10.1016/j.physa.2016.08.002.

[11] Maria Gallucci, "Rebuilding Puerto Rico's Grid," *IEEE Spectrum* 55, no. 5 (May 2018): 30-38, https://doi.org/10.1109/MSPEC.2018.8352572.

[12] Cleo Varianou Mikellidou, Louisa Marie Shakou, Georgios Boustras, and Christos Dimopoulos, "Energy Critical Infrastructures at Risk from Climate Change: A State of the Art Review," *Safety Science* 110, Part C (December 2018): 110-120, https://doi.org/10.1016/j.ssci.2017.12.022.

Social, political, and energy networks do not operate independently but are instead "nested" in one another. Highly resilient social and political bonds are based on activities that cannot operate for long without more fundamental energy and environmental networks. This leaves even the healthiest of social networks vulnerable should supporting energy networks be compromised. As a basic need, utilities such as energy, water, and sewage reflect upon the legitimacy of governing powers, and trust in these institutions quickly weakens when basic services cannot be met. In Kosovo, for example, despite high public trust in the security provided by NATO/KFOR in the country, the electrical utilities KEK and KEDS were publicly maligned and distrusted, and although privatized, still negatively and severely affected public perceptions of government legitimacy and trust in security.[13] In Iraq, US armed forces carried out research that indicated a high correlation with support for the insurgency in those areas of Baghdad (particularly Sadr City) where insurgents had cut access to water, electricity, and sewage.[14] Sparking instability with basic services can be an effective and deniable way to undermine society and leave it more vulnerable. For countries such as Ukraine, with its traumatic experience of the Chernobyl disaster in 1986, the links between energy security and government legitimacy maybe even more fragile.

Attacks and Vulnerabilities in Ukraine

Modern society almost completely depends on the state of security of information and cyber-infrastructure in all spheres of human activity. Not only government structures of states, but also criminal and terrorist organizations have the opportunity to use both information and cyber technologies and information and communication networks to achieve their goals. Motivated by this, the provision of the cyber and information security of the critical infrastructures of the state became a crucial condition for ensuring the state's defense capability and its economic and social development. In January 2018, the US Senate issued a report[15] in which it was noted that, since 2014, Russia has been relentless and diverse in its use of the cyberspace of Ukraine as a cyber art theater and a cyber weapons' testing ground. In many cases, cyberattacks were aimed at the Ukrain-

[13] Mentor Vrajolli, *Kosovo Security Barometer,* Seventh Edition (Pristina: Kosovar Centre for Security Studies, 1 February 2018), http://www.qkss.org/en/Reports/Kosovo-Security-Barometer-Seventh-Edition-1050.

[14] David E. Mosher, Beth E. Lachman, Michael D. Greenberg, Tiffany Nichols, Brian Rosen, and Henry H. Willis, *Green Warriors: Army Environmental Considerations for Contingency Operations from Planning Through Post-Conflict* (Santa Monica, CA: Rand Corporation, 2008), 90-91.

[15] "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations United States Senate, One Hundred Fifteenth Congress, Second Session (U.S. Government Publishing Office, January 10, 2018), https://www.hsdl.org/?view&did=806949.

ian electricity distribution system, disabling for a long time the areas of the economy, infrastructure, and housing. After the Russian attack on the Ukrainian power grid, US officials from the Department of Energy, the Department of Homeland Security, the FBI, and the North American Electric Reliability Corporation increased their involvement. Recognizing the need to study these cyber-impacts, they worked together to understand the tactics and practices of the Russian government, forecast the types of future cyberattacks, and develop effective protection measures against them. Collaboration with Ukraine on countering these threats is also considered a critical element of the United States cyber defense.

The deep penetration of energy in all sectors of the economy and in the social sphere determines its special role in ensuring the security of modern societal development. Energy security characterizes the degree of energy (power) complex performance of its functions in society and the state in ordinary, critical, and extraordinary circumstances.[16] Enterprises and institutions of the energy sector play a leading role in the development of the state.[17] Industry remains the main consumer of electricity, although its share in total electricity consumption in the world is decreasing. Electricity in industry is used to activate various mechanisms and technological processes. Nowadays, the coefficient of electrification of the power drive in the industry is 80%. In this case, about 1/3 of electricity is spent directly on technological needs.[18] The objects of the energy sector are strategically important objects and must function continuously and provide for the delivery of quality services.[19]

On the territory of Ukraine, in each region there are energy structures that belong to the critical infrastructure. Each of them possesses the so-called "critical nodes" which, when disrupted, lead to a breakdown in network functionality and potentially spark cascading failures across networks.

Schematically, this complex is represented in Table 1.

The energy structural elements all relate to a certain hierarchy, control system, and security system. The basis of electricity is the united power system of Ukraine, which centralizes the supply of electricity to domestic consumers, as well as its exports and imports. The system combines eight regional power systems (Dniprovska, Donbas, Western, Crimean, Southern, Southwest, Northern, Central) interconnected by system-generating and interstate high-voltage transmission lines. According to the State Statistics Committee of Ukraine, the largest

[16] Concept of the Development of the Security and Defense Sector of Ukraine, Introduced by the Decree of the President of Ukraine dated March 14, 2016, No. 92/2016.

[17] Cybersecurity Strategy of Ukraine, approved by Decree of the President of Ukraine dated March 15, 2016, No. 96 (Officer Vision of Ukraine, 2016), # 23.

[18] The Law of Ukraine "Basic Principles for the Cybersecurity of Ukraine," No. 2163-VIII of October 5, 2017, http://zakon.rada.gov.ua/laws/show/2163-19.

[19] The National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine, May 26, 2015, № 287/2015, http://zakon.rada.gov.ua/287/2015.

Table 1. Power Complex of Ukraine.

<table>
<tr><th colspan="2">Fuel Industry</th><th colspan="4">Electrical Energy Industry</th><th>Generation Infrastructure</th></tr>
<tr><td colspan="2">1. Coal Mining Industry</td><td colspan="4">1.Thermal Power Stations</td><td>1. Transport</td></tr>
<tr><td colspan="2">2. Gas Industry</td><td colspan="2">State Regional Power Station</td><td colspan="2">Combined Heat and Power Plant</td><td>a) Pipeline</td></tr>
<tr><td colspan="2">3. Oil Industry</td><td colspan="4">2. Hydroelectric Power Stations</td><td>b) Railway</td></tr>
<tr><td>a) Oil Mining</td><td>b) Oil Refining</td><td colspan="2">Hydroelectric Power Plants</td><td colspan="2">Pumped Storage Power Plant</td><td>c) Water</td></tr>
<tr><td colspan="2" rowspan="2">4. Peat Industry</td><td colspan="4" rowspan="2">3. Nuclear Power Plant</td><td>d) Automobile</td></tr>
<tr><td>e) Air</td></tr>
<tr><td colspan="2">5. Shale Industry</td><td colspan="4">4. Alternative Energy Sources</td><td>2. Power Lines</td></tr>
<tr><td colspan="2" rowspan="2">6. Chemical Industry</td><td>a) Wind Power Stations</td><td>b) Solar Power Stations</td><td>c) 3D Alternative PPC</td><td>d) Biofuel Power Stations</td><td rowspan="2">3. Water Supply
a) Control System;
4. Staff Support System</td></tr>
<tr><td colspan="2">e) Fuel Power Station</td><td colspan="2">f) Geothermal Station</td></tr>
</table>

share of electricity is produced in thermal power plants (about 50%), at nuclear power plants (45%), and in hydroelectric plants (5%).

Threats in the Energy Sector

The whole set of threats that can affect the functioning of power systems can be conventionally divided into ordinary threats (probable failures and accidents) and extraordinary threats (these are unique due to the origin, nature of development, and consequences). Various forms of reserving capacities, the development and transportation of fuel and energy resources, systems of guaranteed energy supply, and the creation of reserves of fuel and energy resources serve to counteract unusual threats in power systems. Such ordinary phenomena almost exclude threats to energy security in conditions of the development and functioning of the national economy. In contrast, unusual effects can negatively affect the energy complex as a whole. Among the extraordinary threats, cyber threats play a leading role. Cyber threats are able to provoke such problems as the violation of the provision of energy resources and emergency situations in the power complex of the state. They are implemented in the form of a variety of destructive cyber effects.

Destructive cyber effects can be:

- Targeted attacks (Advanced Persistent Threat)

- Effected on control systems
- Effected through social networks
- Attacks on banking systems (theft of money)
- Hardware bugs (instrument bugs) in chips and firmware of computer and network equipment.

Such cyber threats can be realized by influencing both the entire power complex as a whole and its individual elements separately, as well as with the achievement of synergy of the results. The impact can be carried in a complex, simultaneously, sequentially, or in mixed ways on an automated control system, by personnel, on the financial system of energy, on the hardware and software complex. The most vulnerable place in the united power system is the automated control systems.

An Analysis of Cyber Effects on the Objects of Critical Infrastructure of the Energy Sector in 2014-2018

The issue of cybersecurity of a state energy sector is crucial for national security and defense and for economic and social development.

In 2014-2018, well-planned synchronized cyberattacks were conducted on elements of the Ukraine Power Complex. For a period of time, it gave the violators the opportunity to control the complex and, in some cases, even to destroy both the control system and normal functioning of elements of the Power Complexes. The possible goals of these attacks were, perhaps, to check on the reliability of the cybersecurity system of this state-critical infrastructure, the peculiarities of the cybersecurity system functions of power companies, and their reactions to different cyber effects and incidents. It was shown that an overly complex control over information systems could make power complex objects vulnerable to cyberattacks. The most dangerous cyber effects on objects of power complex are those which provoke, or are accompanied by, destructive chain effects directly onto a power object, which is then connected to other objects of infrastructure and spheres of the everyday life of the nation.

One more peculiarity of the cyberattack on objects of the Ukraine Power Complex was the initial dispersion with final direction on defined systematic multispectral results and diverse effects.

During the analysis of the cyberattacks, it was found that the attacks were not solitary, but were conducted synchronously. All of them had a destructive effect on the automated control system of energy objects. The main synchronous destructive cyber effect was focused on the vulnerable elements of automated control systems. Before the main cyberattack, a preliminary cyberattack was conducted on the service and dispatching system with the purpose of denial of service to consumers. The use of several destructive, concentrated cyberattacks on the power complex was carried out within the framework of a large-scale cyber operation aimed at violating simultaneously several objects of the

power complex of Ukraine.

The groups responsible for many of the Ukrainian cyberattacks, Telebots, BlackEnergy, and Grey Energy, have been closely or more loosely linked to the Russian state by intelligence agencies similar to UK's GCHQ.[20] The lack of any direct attribution, however, does not diminish the strategic use of such tools to destabilize and delegitimate the Ukrainian state. On the contrary, such *maskirovka* approaches to conflict are prime examples of how cyber tools can be used in modern conceptions of hybrid warfare, where vulnerabilities of critical infrastructure are attacked in order to weaken state support and function and increase distrust by potential outside partners. A secondary goal of cyberattacks on energy infrastructure may be to signal to others (e.g., UK, US, Germany) their own vulnerabilities, where Ukrainian attacks serve as proofs of concept. In either case, the activities of cyber attackers are highly coordinated, difficult to trace and attribute, and are highly asymmetrical, non-kinetic attacks. These attacks represent new technical areas of conflict, particularly in cases where an unending state of instability is the goal, rather than the traditional concept of 'total victory' on the battlefield.

One of the important components of the power system in Ukraine is the control system. The control system of the power system plays a leading role in the functioning of the entire energy (power) complex of Ukraine. A powerful cyber effect can be executed on the automated control system, which may lead to a violation of the control of a particular object of energy or the power complex as a whole. The automated control system of the power system should be resilient to cyber effects and have a corresponding Complex Counteract System against cyberattacks.

In December 2015, the Advanced Persistent Threat (APT) was fixed to an automated control system of the power system. The internal networks of the Ukrainian power company Prykarpattya Oblenergo (PJSC) were attacked.[21] As a result of this cyberattack, a large part of the region and the regional center remained without a power supply for several hours. Thirty substations were shut down. About 230 thousand people were deprived of an energy supply for one to six hours. During the attack, the malicious software BlackEnergy was used.[22] The BlackEnergy group launched an attack on the Ukrainian power grid using the BlackEnergy and KillDisk families. This was the latest known use of BlackEnergy

[20] Jack Stubbs, "Hackers Accused of Ties to Russia Hit Three East European Companies: Cybersecurity Firm," *Reuters*, October 17, 2018, https://uk.reuters.com/article/us-russia-cyber/hackers-accused-of-ties-to-russia-hit-three-east-european-companies-cybersecurity-firm-idUKKCN1MR1BO.

[21] Kim Zetter, "Russia's Hacking Attack on the Ukrainian Power System: How It Was," *Texty.org.ua*, http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak.

[22] Bruce Middleton, *A History of Cyber Security Attacks: 1980 to Present* (New York: Auerbach Publications, 2017).

malware in the real world. Following the attack, the BlackEnergy group was found to consist of at least two subgroups: TeleBots and GrayEnergy.

The main goal of the TeleBots group is to implement cyberattacks for sabotage in Ukraine, which is achieved through attacks on computer networks (CNA). This group has committed many devastating attacks, including:

- a series of attacks in December 2016 using an updated version of the same malicious KillDisk software developed for Windows and Linux operating systems
- a known Petya/NotPetya attack in June 2017 with backdoors built into the MEDOC Ukrainian accounting program
- an attack using the BadRabbit family in October 2017.

ESET specialists had been tracking the activity of the GreyEnergy group for several years. The GreyEnergy group uses a unique family of malware. The design and architecture of this malicious software are very similar to the already known BlackEnergy family. In addition to the conceptual similarities of the malicious software, links point to the fact that the group behind the malicious software GreyEnergy closely cooperates with the group TeleBots. In particular, the GreyEnergy team developed a worm similar to NotPetya in December 2016 and, later, an even more advanced version of this malicious program was used by the TeleBots group during an attack in June 2017. It is worth noting that the GreyEnergy group has broader goals than the TeleBots group. GreyEnergy is primarily interested in the industrial networks of various critical infrastructure organizations and, unlike TeleBots, the GreyEnergy group is not limited to Ukraine alone.

At the end of 2015, ESET specialists first spotted the malware GreyEnergy aimed at a power company in Poland. But later, as with BlackEnergy and TeleBots, the focus of the GreyEnergy group shifted to Ukraine. The attackers first showed interest in the energy sector, and then to transport infrastructure and other important targets. The latest use of malware by GreyEnergy was reported in mid-2018.

The GreyEnergy malware is modular, and unlike Industroyer, ESET specialists have not detected any ICS-driven module, meaning that it is targeted specifically at industrial control systems, yet such a system can still be targeted using other methods. At least one case has been detected by the operators of this malicious software deployment. The module can clear the disk to disrupt business processes in a company and hide the traces.[23] One of the most striking details revealed during the ESET study is that one of the detected samples of GreyEnergy was signed by a valid digital certificate, which was probably stolen from a Taiwanese company that manufactures ICS equipment. In other words, the GreyEnergy group literally followed Stuxnet development methods.

[23] "GreyEnergy: A Successor to BlackEnergy," White Paper (GreyEnergy, October 2018), www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf.

Moreover, synchronous attacks were carried out on power companies "Chernivtsioblenergo" and "Kyivoblenergo," but with lesser consequences. On December 23, 2015, an unauthorized group of people interfered with the information technology system of remote access to telecontrol over the equipment of 35-110 kV substations of PJSC "Kyivoblenergo." From 15:31 to 16:30 local time, fifteen cities, towns, and villages were completely or partially blacked out in Myronivsky, Makariv, BilaTserkva, Fastovsky, Skvira, Rokitnyansky, Kaharlyk, Ivankivskyi, and Yagotyn administrative districts. There were over 80,000 consumers without electricity. As a result of the attack, there were failures in the system of remote access; 30 stations, which supply several strategic objects of the region: enterprises, institutions, organizations, and the population, were disconnected. Electricity was restored at 18:56 on December 23, 2015.[24]

The control system was vulnerable to cyberattacks of this kind. The response to such a cyberattack was not timely, and the security system failed to fulfill its functions. With malicious software, a cyberattacker can control and, in certain applications, manage a part of or a whole automated control system. The consequences of such an attack may have been carried out in order to verify the functioning of the security system and the response system to the critical situation of the power company.

In general, the cyberattack was comprehensive and, to a certain extent, systemically organized, by:

- Preliminary infection of networks with the help of counterfeit emails
- Capturing control of the automated control system by executing a shutdown of operations at substations
- Failure of the elements of the automated control system
- Deleting information on servers and workstations (Kill Disk utility)
- Attacking the telephone network of call centers in order to ensure the failure to service to current subscribers.

During the period from January 19-20, 2016, a cyberattack was conducted with the help of the cyber tool Joint Conflict and Tactical Simulation Enhancements, which was also aimed at disrupting the control system by installing malicious software that was sent by e-mail.[25] Another cyberattack, which was carried out during the night from December 17 to December 18, 2016, was less scale-for-effect. The substation "Severnaya" of the power company "Ukrenergo" was disrupted. Consumers in the northern part of the city of Kyiv and the surrounding

[24] "The Largest Cyber Attacks against Ukraine since 2014," *Novoe Vremya*, no. 24, July 7, 2017, https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

[25] "Zillya! Antivirus Has Analyzed the Cyber Attacks on Infrastructure Objects in Ukraine," February 17, 2016, Antivirus Zillya, Certificated for use by public and state authorities, https://zillya.ua/zillya-antivirus-provela-analiz-kiberatak-na-infrastrukturni-ob-kti-ukra-ni.

areas were left without electricity. The attackers did not cause significant damage; the purpose of the attack was a "demonstration of force." As in previous cases, this attack was part of an operation against the state institutions of Ukraine.[26]

The main features of Advanced Persistent Threats are that, as a rule, they:

- are targeted at elements of critical infrastructure
- are conducted by a group of highly skilled hackers
- are carefully masked using specially designed software tools (e.g., specialized Shell Codes, Root Kitta)
- remain unknown for a long time
- are reinforced by intelligence or destructive actions
- and are elements of intelligence and subversive operations.

The analysis of cyber effects is represented in Table 2.

The main cyberattacks differ in their effects and ways of operating. The attacks that were carried out in 2015 on energy companies were not fully self-organized. In 2016, malware that already foresaw self-organization of actions in the process of attacks and actions became more operational. Also, experts from the company ESET, having conducted the research, stated that "Crash Override" was capable of physical destruction of power systems. CrashOverride software[27] has the ability to send commands to the power grid to enable or disable power supply. According to their data, Crash Override can use the known vulnerability of Siemens equipment, in particular, the digital relay Siprotec. Such relays are installed for the protection and control over distribution and power supply networks. Mike Assante, from the American cybersecurity company SANS Institute, has determined that the disconnection of the digital relay can lead to the thermal overload of the power grid. This is a very serious threat to transformers and any equipment that is under voltage. Thus, Crash Override can provide a planned attack on several "critical nodes" of the power complex. Then, there is the probability of a power cut-off on the entire state, as the load moves from one region to another.

Automated power systems of power complexes are vulnerable to cyberattacks. As a result of our analysis of the cyberattacks we can separate out individual categories of possible cyberattacks:

- Target components: electronic computing devices such as Remote Terminals (RTUs) or the Human Machine Interface (HMI)[28] typically have an

[26] Vitaliy Tchervonenko, "Was There an Attack on the Regional Power Company," BBC Ukraine, January 6, 2016, https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc.

[27] Middleton, *A History of Cyber Security Attacks*.

[28] Muhammad Baqer Mollah and Sikder Sunbeam Islam, "Towards IEEE 802.22 Based SCADA System for Future Distributed System," in *Proceedings of 2012 International*

Table 2. Analysis of Cyber Attacks.

Object of effect	Tools used	Way of penetration	Effect	Consequences
2015				
"Prykarpattya Oblenergo"	DoS attack on call centers by the method of "denial of service" to "Oblenergo"[29]	Network Internet	The saturation of the network equipment with a large number of external requests	Consumers could not report about power outage
	Advanced Persistent Threat	SCADA Network, installing malicious software "BlackEnergy"	Interception of the control system in the SCADA network through stolen accounts; sending commands to shut down uninterruptible power systems that have been already reconfigured. After that, shutting down the safety systems leading to interruption of the power supply	About 30 substations were switched off, about 230 thousand people were left without electricity from one to six hours
Chernivtsi Oblenergo	DoS attack on call centers by the method "denial of service" Oblenergo	Network Internet	The saturation of the network equipment with a large number of external requests	Consumers could not report about power outage
	Kill Disk utility	Network Internet	Destroying information on servers and workstations	Failure of IT infrastructure elements
	APT-attack, detection of malicious software "BlackEnergy"	SCADA network	Seizure of control of the Automated Dispatch Systems with the execution	The break in electricity supply was from 1 to 3.5 hours. Total non-delivery of 73

Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, Bangladesh, 18-19 May 2012, https://doi.org/10.1109/ICIEV.2012.6317474.

[29] State Power Company of Ukraine.

			of shutdown operations at the substations	MWh (0.015% of the daily consumption of Ukraine)
"Kiev Oblenergo"	Advanced Persistent Threat	Remote Access System	Unauthorized interference with ACS	Over 80 378 consumers without electricity. The power supply was switched off of 30 node substations, supplying a number of strategic objects, over 80 thousand consumers were without electricity within one to three hours
2016 year				
«KievOblenergo"	Malware Crash Override (the attack was fully automated)	Network Internet	Interception of control of the power system, automated discharging of substations	The substation "Pivnichna" with a power supply for own needs from the substation was completely discharged. Denergized loads of 144.9 MW of PJSC "Kyivenergo" and 58 MW of JSC "Kyivoblenergo". The Kyiv NPP was also discharged with a loss of power for its own needs

interface for remote set up or control. Through remote access, the attacker can intercept the device control and cause malfunctions, e.g., make changes in the data transmitted to the operator, damage the equipment, or produce a complete or partial failure of the device.

- Aim at protocols: nearly all modern data transfer protocols are well documented and their description is open source. For example, the DNP3 standard is common in North American energy control systems.[30] Its

[30] Salman Mohagheghi, Mirrasoul Mousavi, J. Stoupis, and Z. Wang, "Modeling Distribution Automation System Components Using IEC 61850," in *Proceedings of the 2009*

specification is available to anyone at a low price. An attacker can make changes to the information that can lead to significant financial costs due to the overproduction of electricity, switching on the power line during work on them, damage to the equipment, overloading the system.

On June 27, 2017, a large-scale destructive hacker attack ("Petya") was carried out on Ukrainian institutions and organizations. The "critical nodes" of the energy industry (Ukrenergo, Kievoblenergo, Dniproenergo, Zaporizhzhiaoblenergo, and the Chernobyl Nuclear Power Station) also came under direct attack. This cyberattack was aimed at violating the work of company websites and customer support systems. The damage to the information systems of Ukrainian companies was due to the updating of the software intended for reporting and document circulationm M.E.Doc, through installation of a backdoor in the M.E.Doc software update package. Simultaneously with the installation of the update package on the computers of the institutions and organizations, a backdoor was installed, which further promoted the installation of the virus "Petya."

On May 23, 2018, Cisco experts warned about the infection of more than 500,000 routers and systems in 54 countries, but the main goal for large-scale cyberattacks could have been Ukraine.[31] The destructive software "VPN Filter" can be used to conduct such an attack, which allows attackers to intercept all traffic passing through the affected device (including authorization data and the personal data of payment systems), collect and unload information, remotely control an infected device, and even make it out of order. There are also features for monitoring the Modbus SCADA protocols used in automated control systems.

All known cyberattacks that have affected the functioning of critical infrastructure objects in the energy sector have been assessed in the preceding sections.

Conclusion

This article has considered ways and directions for the choice and implementation of rational approaches to solving the complex protection from destructive cyber effects on the state power complex. All major cyberattacks carried out at the Ukraine Power Complex between 2014 and 2018, which influenced the functioning of the objects of critical infrastructure in the energy sector, have been analyzed. It was found that the cyberattacks were not solitary but were conducted systematically. They had a complex destructive effect on energy management systems. It was established that the main destructive cyber effects were concentrated on the vulnerable elements (critical nodes) of the control systems of power complex objects. Before the main cyberattack, a preliminary one was

IEEE Power & Energy Society General Meeting, Calgary, AB, Canada, July 26-30, 2009, https://doi.org/10.1109/PES.2009.5275841.

[31] "Global Ransomware Attack Causes Turmoil," *BBC News Ukraine*, June 28, 2017, https://www.bbc.com/news/technology-40416611.

conducted on the system of maintenance and dispatching, with the purpose of denial to serve the consumers. The use of several destructive, concentrated cyberattacks on the power complex was carried out within the framework of a large-scale cyberattack, which was aimed at simultaneously violating several objects of the energy industry.

It has been established that the system of production and supply of electricity depends on the level of cyber resistance of power objects. An analysis of cyberattacks has shown that the minimum value of the level of stability can lead to the destruction of the power system (object, network).

The methods of realization of hybrid distributed, cumulative cyberattacks with a chain effect on objects of critical infrastructure are described. The vulnerabilities of these objects have been determined. It was established that cyberattacks, which were carried out through e-mail, provided access to the main servers to receive information about the state of the system's operation to intercept the control of objects of the energy infrastructure as a whole, and then to change the parameters of their functioning.

The authors have developed a technique for detecting hybrid distributed-concentrated cyberattacks with chain effects using a model for the intelligent recognition of cyber threats. They have designed, as well, the organizational and technical measures to ensure cybersecurity in the energy sector. It has been shown that systematic measures aimed at the timely detection of cyber threats, preventing and counteracting cyberattacks, will provide the necessary level of functional stability of power complex systems to destructive cyber effects. It will ensure their adequate response to actual and potential threats, rationally using existing capabilities and resources of the state.

Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Authors

Tamara Maliarchuk, PhD, worked for LLC UkrEnergy from 2016–2018. Dr. Maliarchuk was a member of the NATO working group on DEEP program implementation in the Armed Forces of Ukraine. She was an analyst with the S.Korolov Zhytomyr Military Institute in Ukraine and has worked with US forces on language and cyber defense. She conducts research in e-learning, innovative technologies in PTSD detection and therapy, manipulative technologies in web-environment. *E-mail*: maliarchuktamara@gmail.com

Major General **Yuriy Danyk**, Professor, Doctor of Science of Engineering, Chief of Institute of Information Technologies, Ivan Chernyakhovsky National Defense University of Ukraine. He is an expert in the art of war, national defense and security, information and cybersecurity, electronic and IT technologies, robotic complexes design and application, Special forces development. He has combat experience in the application of advanced defense technologies in the conditions of modern war. *E-mail*: zhvinau@ukr.net

Dr. **Chad Briggs** is an Associate Professor and Director of Public Policy and Administration at the University of Alaska Anchorage. Dr. Briggs has field experience in information and hybrid warfare and in developing defensive strategies to protect critical systems in Eastern Europe and the Balkans. He has a PhD in political science from Carleton University in Canada, and has been previously a senior advisor for the US Department of Energy and the Minerva Chair and Professor of Energy and Environmental Security for the US Air University (USAF). He is the author (with Miriam Matejova) of *Disaster Security: Using Intelligence and Military Planning for Energy and Environmental Risks*.
E-mail: cbriggs9@jhu.edu

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Vesna Pavičić, *Connections QJ* 18, no. 1-2 (2019): 111-127
https://doi.org/10.11610/Connections.18.1-2.07

Research Article

Serbia's Orientation Challenge and Ways to Overcome It

Vesna Pavičić

Ministry of Security of Bosnia and Herzegovina,
http://msb.gov.ba/

Abstract: Serbia, the largest country of the Western Balkans, faces a historical choice concerning its future political orientation. Although this choice has been on the agenda since the late 1990s, it will remain unresolved for some time to come. The country's transformation has been moving forward. However, short of integration in western institutions, first of all in the European Union, the process is incomplete and other major players in the international system, first of all Russia but to some extent also China, attempt to influence Belgrade in a direction favorable to their interest. Rational choices in regard to economic integration, trade and investment, and the effects of consolidating democracy should drive Serbia in the direction of the West. However, as demonstrated by some cases, there are factors other than rational choice. Emotional association with Russia, orthodox Christianity, the Russian backing of Serbia in the dispute of the latter with Kosovo, as well as Moscow's sophisticated influence playing on the West's step-by-step advancement and hesitation help Russia better establish itself in Serbia. That results in an inconclusive situation that requires attention to avoid the continuation of hesitancy and uncertainty in the long run. China potentially offers an alternative, primarily as a trade partner and investor. However, its interests in Serbia's future orientation may be different from Moscow's as its investments may offer higher returns if Belgrade becomes a member of the European Union sooner rather than later.

Keywords: European Union, Russian Influence, Serbia, Western Balkans, China.

Creative Commons BY-NC-SA 4.0

Introduction

This article aims to address the historical challenge and dilemma that Serbia has been facing for some time and will face for the years to come. It has to complete its democratic transition as one of the complex challenges. Domestic democratization must go hand in hand with the continuation of modernization as well as continuing alignment with the West and integration in institutions that would further contribute to the consolidation of Serbia's transformation. However, it would be premature to conclude that Serbia has irrevocably settled in the West as it weighs options and some of its partners appear to offer alternatives.

The fundamental attributes of national identity, i.e., "a) historic territory or homeland; b) common myths and historical memories; c) common mass public culture; d) common legal rights and duties for all members; and e) common economy with territorial mobility for members," are playing an important role in Russia's political rhetoric towards Serbia.[1] Ethno-national belonging appears to be the crucial mainstay and differentiation variable of social identification of the members of the largest national communities in Serbia.[2] It is essential to decide which attributes—material or immaterial—matter more in the identity-building. Another important matter is whether those attributes are objective or perceptional, whether they are present in society or being "built" through official and societal discourses. Finally, it is a question of whether external players can contribute to identity-shaping by either directly reaching out to Serbia's society or by influencing its political establishment. If we assume that external players' presence in Serbia plays a major role in shaping the latter's identity, then we have to contemplate which of them is based on what. The political division between its "western" and "eastern" identity continues to be a challenge to the external perception of Serbia as an actor on the international political scene.

Serbia's pro-European orientation has been clearly present since the beginning of the century and the departure of the regime of Slobodan Milosevic from office and power. However, doubts have remained as far as backing the verbal commitment by action and by taking the painful decisions that have been apparently necessary. Hence, the outcome has remained questionable. In 2003, when the EU provided a membership perspective to the Western Balkans, organized criminality demonstrated its power by executing the Prime Minister of Serbia. The assassination of Prime Minister Zoran Đinđić was one of the factors that "influenced a shift in the vector of Serbia's foreign policy towards the East."[3] The responsibility for war crimes of the 1990s was another factor. The fact that many

---

1 Antoni D. Smit, *Nacionalni Identitet* (Belgrade: Biblioteka XX vek, 1998), 29-30.

2 Jovan Komšić, Dragomir Pantić, and Zoran Đ. Slavujević, *Osnovne Linije Partijskih Podela i Mogući Pravci Političkog Pregrupisavanja u Srbiji* (Belgrade: Friedrich Ebert Stiftung, Institute of Social Sciences, 2003), 55-77.

3 Helsinki Committee for Human Rights in Serbia, "The Warp of the Serbian Identity: Anti-westernism, Russophilia, Traditionalism," *Ogledi i Studies* No. 17 (Belgrade, 2016), 188, https://www.helsinki.org.rs/doc/Studies17.pdf.

in Serbia regarded the severe punishments to Serbian perpetrators as "Siegerjustiz" representing a disbalance sentencing Serbs but much fewer Croats and Bosniaks also contributed to the perception of the "unfairness of the West." These are some of the reasons for Belgrade pursuing a declaratory pro-western political orientation without contemplating full engagement and excluding other options. Belgrade's delivery has remained questionable. Today, it is an ambiguously aligned country, where political elites gravitate to different directions and orientate themselves to various power centers.

The countries of the Western Balkans are still facing the challenging process of consolidation. With significant variation, they are often simultaneously interested in engagement with Western states and Russia, while the China factor is also present in their economies. Some of them have completed the process of EU or/and NATO integration, but Russia's influence is visible in their politics. It is more often in doubt whether Russia is also present in their economic sphere. As will be demonstrated later, Moscow's economic engagement is quite limited in terms of bilateral trade with Belgrade (and also with others). However, and this is when one has to return to the question of various attributes of presence and influence, Moscow's presence is highly visible and underlined by symbolism.

Serbia Looks to the EU – The EU Hesitantly Looks Back

Despite that the European Union is "not as attractive as it used to be," Serbia still hopes to join the EU. That was confirmed in 2016 by then prime minister Aleksandar Vučić's statement (now the President of Serbia): "We are rational people and we know this is the best for our country." [4] The Serbian prime minister also stated in 2016 that a "large majority of Serbian citizens favor the continuation of the European path while maintaining close ties with China and Russia." [5] However, the question of how long Serbia would be able to balance between the West and the East without compromising its EU accession prospects still remains. The noticeable disappointment of Serbia is due to a series of factors. Since the democratic transition at the beginning of the century, followed in 2003 by the EU providing "European perspective" to the Western Balkans, occurred half a generation ago. In June 2003, in Thessaloniki, the EU-Western Balkans summit approved the declaration endorsed by the European Council. The declaration stated: "The future of the Balkans is within the European Union. The ongoing enlargement … inspire and encourage the countries of the Western Balkans to follow the same successful path." [6] Although the EU's commitment remained

[4] More on this matter: "Vucic Says EU Membership Has 'Lost Magic Power' for Balkans," *Radio Free Europe/Radio Liberty*, February 23, 2016, http://www.vucic-says-eu-membership-has-lost-magic-power-for-balkans-migrant-crisis-brexit.

[5] Reuters online: https://www.reuters.com/article/us-serbia-election/serbias-vucic-confirms-domination-with-presidential-win-idUSKBN1733VI.

[6] Declaration, EU–Western Balkans Summit, C/03/163, Thessaloniki, June 21, 2003, 10229/03 (Presse 163), point 2.

vague and did not mention any timeline, still some states in the Western Balkans must have been under the impression that the perspective will be realized faster.

A decade later, when the EU Commission of Jean-Claude Juncker was formed, the incoming Commission President stated the following: "In the next five years, no new members will be joining us in the European Union. … However, the negotiations will be continued and other European nations and European countries need a credible and honest European perspective. This applies especially to the Western Balkans."[7] Five years have passed, and with the Commission leaving office, it can be stated that if there was one promise that Juncker held, it was that there was no further enlargement of the EU during those five years. Closer to the end of the office term, the EU may have noticed that the absence of tangible enlargement prospect reduces EU influence in the region and only increases the influence of other powers. Hence, a Communication issued in February 2018 reaffirmed the vague promise in somewhat clearer terms: "Accession negotiations are already well underway with Montenegro and Serbia. With strong political will, the delivery of real and sustained reforms, and definitive solutions to disputes with neighbors, they could potentially be ready for membership in a 2025 perspective. This perspective is extremely ambitious. Whether it is achieved will depend fully on the objective merits and results of each country."[8] Formally, EU enlargement hardly got closer and that makes the doubts of politicians, diplomats, NGOs, and scholars concerning the accession of any country of the Western Balkans to join the EU by 2025 understandable.[9]

Certain developments indicate no breakthrough as far as enlargement in the Western Balkans. The number of chapters closed or opened in the accession talks with Belgrade has risen to two provisionally closed and 17 opened chapters out of 35.[10] As the negotiations have been going on since 2014, this illustrates piecemeal advancement. However, it is important to mention that economic re-

---

[7] Jean-Claude Juncker, Candidate for the President of the European Commission, "A New Start for Europe (Speech/14/567)," Strasbourg, July 15, 2014, http://europa.eu/rapid/press-release_SPEECH-14-567_en.htm.

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A Credible Enlargement Perspective for and Enhanced EU Engagement with the Western Balkans," Strasbourg, February 6, 2018, COM(2018) 65 final, https://ec.europa.eu/commission/sites/beta-political/files/communication-credible-enlargement-perspective-western-balkans_en.pdf.

[9] Julija Simić, "Serbia in the EU in 2025 – Mission (Im)possible," *Euractiv.rs*, April 5, 2019, https://www.euractiv.com/section/enlargement/news/serbia-in-the-eu-in-2025-mission-impossible.

[10] As of the end of May 2019. See Commission Staff Working Document, *Serbia 2019 Report*, accompanying the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2019 Communication on EU Enlargement Policy," COM (2019) 260 final, Brussels, May 29, 2019, SWD(2019) 219 final, 4, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-serbia-report.pdf.

lations have also intensified. As of 2017, the EU is Serbia's single largest trade partner, representing more than 60 percent of both its export and import. Its trade exceeds every other partner's by almost 8:1 ratio in import and 11:1 ratio in export compared to the second largest. Regarding import, Serbia's second-largest partner is China (8.1 percent); in export, it is the Russian Federation (5.9). In sum, the EU has no alternative in the external trade of Serbia. The situation is even more tilting in the direction of the EU as far as the inflow of foreign direct investment (FDI) in the period 2010-2017, representing approximately 73 percent of the total. The second-largest investor is Russia, representing less than 10 percent. The cumulative FDI of the EU is seven and a half times higher than that of the Russian Federation.[11] In sum, if we assess Serbia's situation exclusively based on economic rationality, the EU has no alternative. However, this information should reach the large portion of the Serbian population that may be affected by other considerations, influenced by messages addressing emotions and solidarity with reference to identity matters. Moreover, even on purely economic considerations, it has to be taken into account that some of the trade, FDI, and other kinds of acquisition is concentrated in certain strategic branches of the economy like energy (Russia) and telecommunications (China) that may affect the perception of economic dependency.

It is also important to note that the EU commitment to Serbia as a candidate country is going beyond trade and investment. Namely, Serbia is the "largest recipient of EU donations in the Western Balkans and one of the largest in the world."[12] This is understandable in light of the fact that Serbia is the largest economy and the most populous country of the Western Balkans, and it is difficult to imagine a next EU enlargement in the region without Belgrade's accession. The European Union is the biggest donor of Serbia "with more than EUR 3 billion in non-refundable aid over the past 15 years, … and the country's number one partner in supporting development and ongoing reforms." The grants provided over the past 15 years aimed to contribute to development in all fields, ranging from the rule of law, public administrative reform, social development, education, environment, the improvement of the infrastructure, and agriculture.[13]

It is clear that there are problems with Serbia's advancement to EU membership on both sides. The most important among them are listed below:

1. The EU's hesitation is due both to factors that stem from Serbia's situation and others that are unrelated. As far as Serbia is concerned, it certainly does not

[11] The Delegation of the European Union to the Republic Serbia, FDI to Serbia, Imports to Serbia, Exports from Serbia, http://europa.rs/serbia-and-the-eu/trade/fdi-in-serbia/?lang=en; http://europa.rs/serbia-and-the-eu/trade/serbia-total-imports/?lang=en; http://europa.rs/serbia-and-the-eu/trade/serbia-total-exports/?lang=en.

[12] The Delegation of the European Union to the Republic Serbia, "EU and Serbia at Work," http://europa.rs/eu-assistance-to-serbia/eu-and-serbia-15-years-of-partnership/?lang=en.

[13] The Delegation of the European Union to the Republic Serbia, "EU and Serbia at Work."

help that the country's lasting political orientation, including the anchoring of the country in the West, is not so unequivocal as was in the case of East-central European states when they first demonstrated their aspiration to settle in the West and become EU (and NATO) members in the 1990s. The country's international political orientation should be exempted from party politics, at least as a strategic objective. There are other matters where improvement could be more persuasive, such as reducing the level of corruption, good governance, and others.

2. The EU's hesitation is also due to matters not related to Serbia. The late-1990s period was characterized by enthusiasm in European politics; politicians were under the impression that Europe is on the way to unification and lasting peace. At the end of the 2010s, many in Europe are skeptical, Europe gives the impression of a re-divided continent, and the Western Balkans may be the last unsettled area in addition to some former Soviet republics (Ukraine and Georgia). There is no lasting peace on the European continent. There is a geopolitical rivalry between the West and Russia. Also, some new EU members that joined since 2004 did not deliver particularly well on their promises. Checks and balances are not respected, the judiciary's independence is violated, human rights are undermined by measures like the domination of the media by a few loyal actors and cronies, political power is used for the enrichment of members of the political establishment, and the unceasingly high level of corruption, among others. Understandably, the EU does not want to make another big mistake and integrate states that do not deliver on promises after gaining membership. The EU does not want to see further members, which regard membership as a "cash cow" while not delivering on some of the foundational values of the Union and taking solidarity on critical matters.

The fact that the EU has managed the Western Balkans enlargement as a routine matter since the issuance of the February 2018 document has been due to various factors. It is the single most important reason that the EU was busy with other matters ranging from BREXIT to the discord concerning migration and some notorious members challenging agreed values. Furthermore, the change of guard in several leadership positions, including the EU Commission, the European Parliament, the European Council, and the European Central Bank, diverted the attention away at least temporarily. In parallel, the so-called Berlin mechanism, dedicated to addressing the Western Balkans, has been fading due to Germany's diminishing commitment. Whether the EU under the new leadership will make enlargement in the Western Balkans a priority remains to be seen.

Serbia has strong reservations towards NATO underlined by the 78 nights of bombardment in March-June 1999. It is also a country that regularly reasserts to keep its neutrality. However, this does not mean that it has no relations with the Atlantic Alliance. It participates in Partnership for Peace (PfP), has signed an Individual Partnership Programme (IPAP), and joins exercises with NATO member states. Hence, it can be concluded that Serbia has been pursuing a vectoral foreign and security policy within limits. While Serbia's NATO membership is not a

current issue and the situation will not change any time soon, it is a question whether Belgrade's security situation could be influenced in any other manner. There is one regional issue that is closely linked with Serbia's security. Namely, as Belgrade approaches the EU and will possibly become an EU member in the next decade, the problem is how to avoid a sharp divide between Serbia and Bosnia and Herzegovina. It is clear that with its current performance and constitutional system, Sarajevo cannot become an EU member. However, if Belgrade becomes an EU member without any perspective for Bosnia and Herzegovina, the Bosnian Serbs will have two options: to become Serbian citizens as individuals or join Serbia with the territory of the Republika Srbska. Although NATO membership would not resolve this problem, it might alleviate it.[14]

Similar to earlier enlargements, it is essential to keep the strategic importance and political attention since, without it, the drive will dissipate in the hands of technocrats. This has already been the impression of various forces in the Western Balkans.[15] A strategic approach would probably contribute to draw-different conclusions regarding the timeframe and some of the detailed conditions of accession. However, it raises a delicate question: To what extent should the EU compromise accession conditions in the name of recognition that it is part of a geopolitical rivalry first of all with the Russian Federation. This also raises the question of to what extent the candidates could instrumentalize the strategic importance of enlargement and hence change the discourse to their advantage. It is certain that both parties are aware of the dilemma and regard the approach to enlargement as an instrument.

Russia's Counter-interests and Its Means

The Russian Federation has never left the Western Balkans. Its presence has been steady, although its intensity, emphasis, and ramifications of Russian politics have changed since the 1990s. Ever since the wars in former Yugoslavia came to an end, the Russian interest focused on a continuing commitment without sacrificing large material resources or, for that matter, the best people over there. This attitude may be due to the recognition that the small and medium-size states of the Western Balkans are less important than the great powers with which Moscow identifies itself as being in the same league or the traditionally higher importance assigned to the other successor states of the Soviet Union.

The relations between Russia and the Western Balkans are based on similar foundations:

[14] I do not deny that such a solution is "the second best." It would be certainly better to overcome the legacy of Dayton and put Bosnia and Herzegovina on the road to EU membership. However, this may be an illusion under the current conditions.

[15] For the best overview of such a position see European Movement Serbia and Embassy of the Federal Republic of Germany in Serbia, "Twelve Proposal for EU Enlargement from the Western Balkans" (Belgrade, June 2018), http://www.emins.org/wp-content/uploads/2018/06/Twelve-Proposals-web.pdf.

1. Political engagement is based on different discourses in accordance with the expectations of the receiving country and its population.
2. Identity politics is an essential part of it. In Croatia, it is about Slavonic roots; in Serbia, this is complemented with an emphasis on Orthodox Christianity, and the same goes for the Serbs in other countries of the region.
3. The Russian presence and contribution are amplified by tailor-made media messages. Russia has invested in this by the Serbian language news program of RT and Sputnik news. The latter is reaching out to communities in various languages. They often support the politicians in power in the respective states, undermine the credibility of the opposition, speak about their brutality when rebelling,[16] and attempt to alienate the population from the West.[17]
4. Distortion of history also plays a role, including the presentation of an exaggerated role of the Soviet Union in the liberation of Yugoslavia in World War II. The difficulties that characterized Soviet-Yugoslav relations of the late-1940s are erased from history, whereas Russian support to Serbia in the Dayton peace arrangement and even more in the so-called Kosovo war of 1999 are often emphasized.
5. The Russian-Western Balkans relations are often visualized by symbolic high-level meetings in the Croat, Serbian and Bosnian Serb context. This includes presidential meetings, including a high profile visit of President Putin to Serbia in 2019. Such a visit is of high-visibility and includes liturgical elements.
6. In the Serbian context, a state that, unlike most states of the Western Balkans, is neither member of NATO nor approaching it, cooperation has an important symbolic military component, including Russian military assistance.
7. Russian political support also extends to Serbia as far as its claim of Kosovo belonging to Serbia.
8. The Russian economic footprint is relatively small overall. Western Balkans' trade with Russia equals approximately 4 percent of the total, including 3.1 percent of export and 4.9 percent import.[18]

---

[16] See the report of RT on the behavior of anti-government protesters in Belgrade: "Serbian Anti-govt Protesters Break through Police Cordon & Block Presidential Palace," *RT*, March 17, 2019, https://www.rt.com/news/454071-serbia-vucic-protest-police/.

[17] It suffice to mention the extensive reports of Sputnik News on wide-spread lewd behavior in the West, including homosexuality and nudity, that intend to alienate many Muslims. See https://sputniknews.com/tags/tag_Albania/.

[18] See Eurostat, "Western Balkans Countries-EU – International Trade in Goods Statistics," *Eurostat: Statistics Explained*, May 2019, https://ec.europa.eu/eurostat/

In sum, the Russian presence in the Western Balkans has a mixed foundation, including the strengths and weaknesses listed above. Serbia belongs to those states which, due to size, historical and religious links (and some of its mystification), and its pending Kosovo dispute, attract the prime attention of Moscow. With this, an impression is created as if Moscow would present an alternative for Belgrade. If we take a closer look at some of those factors, the picture becomes more nuanced.

1. The relatively low intensity of economic relations between Russia and the Western Balkans generally and with Serbia specifically, in terms of both trade and investment, does not mean Russia's insignificance in the relationship.

- In Serbia, Russian-owned or indirectly linked firms control close to 13 percent of the national economy's revenues.
- Direct dependence is complemented by indirect elements, like dependence on Russian raw materials, export to Russia, and debt for gas supply.
- Serbia is heavily dependent upon gas supply by Gazprom and largely dependent upon oil supply by Lukoil. Local political intermediaries prevent the diversification of the energy markets.
- Gas dependence will further increase due to transit linked to the continuation of Turkish Stream and cooperation with Russia in supplying parts of Serbia with liquefied natural gas where pipelines do not reach habitations.
- Russian loan schemes contribute to the dependency.[19]
- Russian state-owned Sberbank entered Serbia's market in 2012 and purchased the "banking arm of Volksbank International in Central and Eastern Europe."[20]

2. The Russian connection is highly visible in military matters. Serbian officers study at Russian defense academies. The Serbian military conducts exercises with the Russian military. Since 2013 Serbia has observer status with the Collective Security Treaty Organization (CSTO) and has a "military cooperation agreement with Russia in place which allows Russian soldiers to be based at Niš airport."[21] Last but not least, Serbia has received Russian armaments and equipment from Russia, including BRDM-2 reconnaissance and patrol vehicles, T-72 battle tanks, and MiG-29 combat aircraft. Even though this looks impressive, in

statistics-explained/index.php?title=Western_Balkans-EU_-_international_trade_in_goods_statistics&oldid=480316.

[19] Centre for the Study of Democracy (CSD), "Assessing Russian Economic Footprint in Serbia," *Policy Brief* no. 72, January 29, 2018, https://csd.bg/publications/publication/policy-brief-no-72-assessing-russias-economic-footprint-in-serbia, 1.

[20] CSD, "Assessing Russian Economic Footprint in Serbia," 12.

[21] Official site of the Ministry of Defence of Republic of Serbia, http://www.mod.gov.rs/lat/11655/unapredjenje-standarda-i-modernizacija-vojske-prioriteti-ministarstva-odbrane-11655.

fact, they are fairly dated pieces, and in the case of the MiG-29s the modernization costs have to be borne by Serbia.

3. Russia gives diplomatic backing to the power holders in Belgrade that is essential when the leadership is challenged. Although this is expressed in somewhat ambiguous terms, like when Russian Foreign Minister Sergey Lavrov confirmed that Russia is extremely interested in the long-term stability and prosperity of the entire Western Balkans region, it has still been pronounced.[22] This could only be regarded as a cynical statement just a few months after the Russian Federation attempted a *coup d'etat* against the elected leaders of Montenegro, and while it made attempts to drive wedges between political forces in (as it is now called) the Republic of North Macedonia. However, Russia is certainly interested in the stability of Serbia as it is unlikely that instability (or any turbulence) would be to Moscow's benefit.

Taken together, the Russian Federation lastingly intends to remain part of the Western Balkans equation. Its attention focuses on states, which have not been firmly anchored in the West regarding institutional alignment in the EU and NATO. Other factors, like the economic possibilities, certainly also play a role, e.g., it has kept Russian interest in Croatia as an investor in the agroindustry and elsewhere. Serbia is at the intersection of these two factors. Russia's primary intention is to prevent the completion of the western integration of the entire region. Towards that purpose, Moscow uses various means, including fully legal, morally questionable, illegitimate, and outright illegal ones. With such a combination of various means, it has succeeded in contributing to the impression that Serbia is not a lastingly and irrevocably settled country as far as its political orientation. With its limited means, this is the maximum that Russia may hope to achieve. With limited means, it is difficult to be a major positive contributor. However, it may be sufficient to be a spoiler, in particular when the West continues to be hesitant in expeditiously moving forward with completing the Western Balkans' integration.

China as a Complementary Complicating Factor

The Russian Federation is an actor that, lastingly and by a complex set of means, attempts to influence Western Balkans' politics. This is understandable, as it regards the region as the last unsettled area of Europe. Russia has difficulties accepting that some sovereign states in the area of the former Soviet Union may also like to define their own future rather than accepting Russia's tutelage. Although the Western Balkans' gradual approach to the West is undeniable, as long

[22] Ministry of Foreign Affairs of the Russian Federation, "Foreign Minister Sergey Lavrov's remarks and answers to media questions at a news conference following talks with Deputy Prime Minister and Minister of Foreign and European Affairs of Croatia Davor Ivo Stier, Moscow, May 23, 2017," www.mid.ru/en/web/guest/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/2763697.

as the process is not completed, Russia feels to have a chance to strain its muscles.

China had no particular interest in the region after the break-up of Yugoslavia. However, with its global economic expansion that finally reached the whole of Europe during the last years of the 2010s, when due to the global financial crisis, the old continent became more attractive, the Western Balkans also reached China's attention threshold. With the One Belt One Road (now Belt and Road) Initiative and later with 16+1 (17+1), explicitly dedicated to East-central and South-eastern Europe, China has taken more active interest. The interest has remained focused on the economy and does not seem to go beyond the economic relaitons. Of course, economic interaction is dependent on political stability. The view that Beijing gives preference to cooperation with political systems that are similar to China's is widespread in the West, yet difficult to substantiate. Nevertheless, there is evidence that:

- China, as a trading and investment partner, is more corrupt than most western economies;
- China prefers inter-governmental relations in its transactions and creates lasting dependencies that make it interested in lasting political stability;
- The majority of its enterprises are state-owned, whereas the 35 percent share of privately-owned companies (that does not include the largest ones) are also dependent upon the Chinese political authorities.

In the Western Balkans, the concerns emanating from the previous points, including that many politicians in the region are not immune to corruption, are complemented by the size of the economies. They may easily become dependent upon a large partner, like China, as an investor and a loan provider. China is a mixed blessing for the non-EU members in the Western Balkans as Chinese investment does not have to meet the EU requirements to reduce financial opaqueness, contribute to transparency, and meet certain standards as far as profitability and environmental concerns. The experiences of some countries in South Asia and Africa should serve as warning signals.

The situation varies from country to country in the Western Balkans ranging from highly indebted Montenegro with 78 percent of its sovereign debt per GDP to Serbia, where it reaches only 12 percent. Serbia attracted more than 2.5 billion euro Chinese projects, among which the largest is the modernization of the railroad connection between Belgrade and Budapest,[23] a project surrounded by doubts as far as profitability. However, as it is also representing 44 percent of the region's non-EU economies, it is less endangered to be dominated by China than its smaller regional partners. It seems Belgrade is fairly careful with Chinese

[23] Valbona Zeneli, "China in the Balkans: Chinese Investment Could Become a Challenging Factor for the European Future of the Western Balkans," *The Globalist,* April 9, 2019, https://www.theglobalist.com/Balkans-china-fdi-belt-and-road-eu.

investment and loans that it regards as expressions of neo-colonialism. It remains to be seen whether this will change in light of the Chinese promises and the adoption of two relevant Chinese documents, the Guiding Principles on Financing the Development of the Belt and Road Initiative and the Debt Sustainability Framework for Participating Countries of the Belt and Road Initiative.[24] Although China did not recognize Kosovo's declaration of independent statehood, its presence in Serbia (just as generally in the Western Balkans) has retained its economic focus and the Chinese support to Serbia did not become highly visible. Although this might change in the future, it is necessary to note that the economic aspect is currently the nearly exclusive focus of China's advancement in the Western Balkans. Beijing's growing overall influence without a major change in its policy and without far more direct EU influence may create problems as far as the spread of good governance in the Western Balkans. This may in turn undermine the chance of EU enlargement and its benefits both for the EU and the inhabitants of the states of the Western Balkans.

The Kosovo Quagmire: An Aggravating Factor

Kosovo moved from *de facto* to *de jure* independence with its declaration of independent statehood in February 2008, recognized by many[25] as Belgrade could no longer credibly argue for multi-ethnicity. Serbia has not been able to find a solution to this matter in cooperation with Kosovo. As Belgrade is not in the position to officially take note of Kosovo's independence, it has retained its revanchist attitude. That does not mean it would be ready to use forceful means to reverse the status quo. Yet, for Serbia, the issue is undecided. History teaches us that states with revanchist aims (except for the world's strongest powers) usually try to find support for their aspirations. This creates allegiances and dependency on their supporters. Many states fell into this trap in history and paid dearly for their mistake. As the Russian Federation has openly supported Serbia in its aspiration to "regain" its territorial integrity, Moscow has contributed to a dependency that both states find advantageous. If we go back to the roots of the matter, it is clear that UN Security Council Resolution 1244, adopted upon the end of the Kosovo war, left ambiguity concerning the territorial status of Kosovo.[26] This was due, among others, to the essential contribution of the Russian Federation to bringing about a resolution that entailed the end of the military conflict fought by NATO against Belgrade.

---

[24] Amine Bennis, "China's Inroads into the Balkans," *The World Today* (Chatham House, June-July 2019), https://www.chathamhouse.org/publications/twt/china-s-inroads-balkans.

[25] Overall, during the first ten years after the declaration of independence (February 2008) 117 states recognized Kosovo. See https://www.kosovothanksyou.com.

[26] Resolution 1244 (1999), adopted by the Security Council at its 4011th meeting, on June 10, 1999, S/RES/1244 (1999), https://digitallibrary.un.org/record/274488.

Russia's veto power in the UN Security Council used to block the furthering of Kosovo's statehood made Serbia's foreign policy linked to Russia. In 2008, the Serbian government decided that its policy priorities would be the preservation of the country's territorial integrity, meaning also the retention of Kosovo, and also EU integration. Such an approach contributed to creating "a two-vector foreign policy," which represents bipolar communication "balancing between Brussels and Moscow, and it became the constant of all Serbian governments."[27] Regardless of "its official commitment to EU integration, the Serbian Government … continued to pursue the foreign policy of both EU and Russia."[28]

The progress of normalization has remained somewhat inconclusive. Serbia and Kosovo signed two agreements towards normalizing ties upon strong encouragement and facilitation of the EU. "Following the EU brokered deals in 2013 and 2015, relations with Serbia seem to be normalizing, but independence did not necessarily bring about democratic and accountable governance."[29] EU officials assessed the signing of the agreements in Brussels as "the key step in normalizing relations between Serbia and Kosovo, but also as mandatory precondition for move along to EU integration."[30] The EU's influence continued to bring Serbia and Kosovo to the negotiating table. However, in January 2018, the leader of Serbs in Kosovo was gunned down in Mitrovica on the day talks should have restarted between the two parties.[31] This has indicated opposition to the reconciliation process. The ambiguous declaration of the EU reflected in the press as some vague promise that Serbia and Montenegro may become members of the Union in 2025 had an impact on the parties.[32] Kosovo could conclude that the settlement of its status through its recognition as an independent state will be more urgent to Belgrade, as it is apparent that Serbia cannot become an EU member without it. As we know, the party feeling the urgency would be more willing to seek compromise. This resulted in miscalculation. To make the long story short, Belgrade continued to block Pristina's membership in certain international organizations, whereas the latter introduced a hundred percent customs duties for Serbian and Bosnian and Herzegovinian products that *de facto* meant that they had no chance in the market in Kosovo. Finally, to facilitate a sustainable solution, the idea has emerged to resolve some of the contentious

[27] Helsinki Committee for Human Rights in Serbia, *The Warp of the Serbian Identity*, 191.

[28] Helsinki Committee for Human Rights in Serbia, *The Warp of the Serbian Identity*, 191.

[29] Lana Pašić, "Democracy, 25 years after Yugoslavia," *openDemocracy*, April 3, 2016, https://www.opendemocracy.net/can-europe-make-it/lana-pasic/democracy-25-years-after-yugoslavia.

[30] Dušan Vučićević, "Parlamentarni Izbori u Srbiji 2016," *Političke Analize* 7, no. 25 (2016), 26.

[31] John R. Schindler, "Mysterious Balkan Assassination Threatens Regional Peace," *Observer*, 16 January 2018, http://observer.com/2018/01/assassination-of-oliver-ivanovic-threatens-peace-in-balkans.

[32] Communication from the Commission to the European Parliament, "A Credible Enlargement Perspective," point 5.1.

issues between Serbia and Kosovo by exchanging territories. However, this would mean a departure from the position of the so-called Contact Group held since the early years of the 21st century. There are countries, which actively support such a solution, like the United States; others, like France, are hesitant, and some fear chaos, e.g., Germany. The matter is also divisive in domestic politics as some leaders support it, such as the President of Kosovo, while others, like the country's long-time prime minister, opposed it. Short of consensus, the matter remains without resolution.

The Russian Federation never said it would not recognize the statehood of Kosovo; rather, Russia expressed the view that it would join an arrangement that Serbia finds acceptable. In the second half of the decade, Moscow started to notice that solving the matter of Kosovo statehood may be approaching. This would reduce Russian influence in the Western Balkans. Moscow initiated a variety of measures in order to prevent this unfavorable development. Russia offered its readiness to mediate between the parties in order to undermine the EU monopoly in Serbia-Kosovo relations. However, it was apparent that Russia only wants to delay the process and gain influence. Moscow also started to promote the withdrawal of recognitions to Kosovo's statehood actively. Overall, in the second half of the 2010s, 14 small states withdrew Kosovo's state recognition. This has been regarded as a success in Belgrade, while Russia, understandably, did not advertise its role in the process.[33]

During the first half of the 2010s, Serbia's government measured the change of public opinion and considered if and when the recognition of statehood could be offered to Kosovo.[34] In July 2015, 72 percent of the Serbian population believed that Serbia would be compelled to recognize Kosovo in order to join the European Union, while 57 percent held the view that Serbia should refuse to accept that even if it means staying out of the EU. The population's decreasing will to join the EU is shown in the following statistic: 76 percent supported EU integration in October 2009, 71 percent in August 2010, 69 in April 2011. By November 2015, this percentage decreasing to 49.[35] Surveys conducted in 2019 show that 78 percent of the respondents would not support the decision to recognize Kosovo's independence in exchange for Serbia becoming an EU member faster. At the same time, 27 percent of the respondents think that the government of Serbia will recognize Kosovo's statehood. These findings are particularly interesting, given that 47 percent of the respondents think that Kosovo has been

[33] The website listing the recognitions of Kosovo provides no information of the recognitions withdrawn. See www.kosovothanksyou.com.

[34] Centre for Insight in Survey Research, "Survey of Serbian Public Opinion: November 24 – December 3, 2015," http://www.iri.org/sites/default/files/wysiwyg/serbia_november_2015_poll_public_release.pdf.

[35] Centre for Insight in Survey Research, "Survey of Serbian Public Opinion."

lost for Serbia.[36] It is important to closely follow the tendencies as Serbian politicians may be reluctant to put their future at risk at the price of recognizing Kosovo, while it is hard to imagine the continuation of the EU enlargement process with Serbia without such recognition. However, the monitoring of the public opinion may not matter exclusively for Serb politicians, but EU officials and politicians of the member-states as well. It would result in a strange situation if, close to the accession talks, the EU "wakes up" and concludes that the population of Serbia (and hence the political class) is reluctant to pay the price for the accession by recognizing the *de facto* territorial status quo.

Ways to Mitigate This Dilemma – Conclusions

Bearing in mind Serbia's still existing orientation toward the European Union, the integration process should be accelerated. Efforts by both sides, EU and Serbia, should be focused on increasing understanding of democracy and European identity. The political dialogue needs to be intensified in security, political, and economic frameworks for developing Serbia's security and socio-economic system in a clear direction. The development of the country, increasing the standard of living, providing for more transparency and freedom of the press, changing political rhetoric will eventually facilitate the transition process and EU integration.

Strengthening civil society's role in free media promotion and protection will weaken hate speech and obstructions to democratic processes. "The role of media is central in the life of many people in Serbia …" and the European Union should use mechanisms to support "free and independent media in Serbia, as well as bringing back (or indeed introducing) to the country international media outlets."[37] The role of the media in building public opinion is unquestionable. Also, investment in adequate education of the youth will prepare future generations to understand democratic standards and preserve them.

Even the fact that "the Serbian public has expressed its dissatisfaction with EU conditionality," the European Union should bring back its reputation and "clarify Serbia's requirements regarding Kosovo" and "accommodate sensitive issues in Serbia in the accession process,"[38] otherwise, Russia and China would show the broader interest to improve their "unconditional" cooperation. More flexibility and clear dialogue regarding critical issues could allow progress. Europe should consider the possible consequences for Europe more seriously due

[36] "Većina građana Srbiji smatra da je Kosovo traino izgubljen," *SEEbiz,* March 31, 2019, accessed November 23, 2018, http://rs.seebiz.eu/vecina-gradana-srbije-smatra-da-je-kosovo-trajno-izgubljeno/ar-191944.

[37] European Parliament, "Serbia's Cooperation with China, the European Union, Russia and the United States of America," EP/EXPO/B/AFET/2017/09 (Directorate-General for External Policies, Policy Department, November 2017), 44, https://www.europarl.europa.eu/cmsdata/133504/Serbia%20cooperation%20with%20China,%20the%20EU,%20Russia%20and%20the%20USA.pdf.

[38] European Parliament, "Serbia's Cooperation with China," 45-47.

to the presence of different geopolitical interests in the Balkans rather than creating strict, often technical conditions for membership. Further delay of the integration of all remaining Western Balkan countries could result in the loss of the region. However, the states of the western Balkans, which aspire for EU membership, should also find ways to more effectively fight those phenomena that form obstacles to EU membership (including corruption and weak governmental capacity).

Continuous tensions in the region demand intensive engagement and a stronger presence of the United States, but also the encouragement of the European Union for the accession of Western Balkan countries. United States programs to strengthen economic growth, the rule of law, and fight against corruption remain important for the Euro-Atlantic integration of the region,[39] but insufficient. Strengthening political dialogue and the more active engagement of the US leadership in the Balkans is much needed.

Therefore, it could be another possibility that "the EU and U.S. need a joint strategy which should include common policy to address regional security threats, clear EU and NATO membership perspective as well as the development of a common energy policy."[40] Currently, this may be problematic as the US and the EU, as well as some EU larger members, have many other divisive issues on the agenda that would make it difficult to overcome and refocus the attention to the Western Balkans. However, the US seems to have a clear idea how to overcome the Serbia-Kosovo stalemate, and its contribution may be indispensable over there. The common interest of the West and the Western Balkans countries should be to support stability, economic development, democratic transition, and re-empowering integration in the EU.

A secure environment may contribute to an increase in foreign investment, which would positively impact development. The state should increase public awareness regarding the importance of the EU and its benefits and implications on Serbia's future socio-economic development. Serbia's EU integration is also urgent in protecting it from a foreign intervention that would lead the country and, with it, the region into political stagnation and isolation. Today Serbia's foreign policy relies on four major external powers: the European Union, the United States, the Russian Federation, and China. In the short-term, Serbia can sustain an "unstable equilibrium." However, further progress towards EU accession could mean that Serbia will have to "sacrifice some independence in foreign af-

[39] John McCain, "The Balkans Are Heating Up Again - and Washington Is Nowhere to Be Seen," *The Washington Post*, April 27, 2017, https://www.washingtonpost.com/news/democracy-post/wp/2017/04/27/the-balkans-are-heating-up-again-and-washington-is-nowhere-to-be-seen/.

[40] Ernst M. Felberbauer and Predrag Jureković, "A Region in Limbo: South East Europe in the Light of Strained Western-Russian Relations," Study Group Information Band 26/2015 (Republic of Austria, Federal Ministry of Defense and Sports, September 2015), https://www.bundesheer.at/wissen-forschung/publikationen/publikation.php?id=936, 114-115.

fairs."[41] The EU, in turn, should find ways to be far more visible in Serbia, and in the Western Balkans more broadly, and "sell better" its essential contribution to the development of the region.

It is essential to understand Russia's role in attempting to destabilize the Balkan region that is hidden behind the pan-Slavic political rhetoric. Russia's excellence in shaping the identity of Serbia's population could be a message to the European Union about its ineffectiveness and inability to do the same. The strategic partnership "justified" on the basis of economic cooperation is not realistic in light of the distance between Serbia and Russia, and also due to the fact Serbia already conducts most of its trade and foreign direct investment with the EU countries.

If Serbia wishes to join the European Union, balancing between Brussels and Moscow has to be stopped. "The Western Balkans has become part of the new geopolitical competition."[42] The European Union's foreign policy is the one that should be followed. On the other hand, Brussels should do its best not to allow further Russian obstruction of European and Euro-Atlantic integration in the future. Russia's strength in Serbia is the EU's weakness.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Vesna Pavicic is a civil servant in the Ministry of Security in Bosnia and Herzegovina. Since 2018 she has been serving in the OSCE Special Monitoring Mission (SMM) in Ukraine.

[41] European Parliament, "Serbia's Cooperation with China," 1-38.

[42] Felberbauer and Jureković, "A Region in Limbo," 114.

Connections: The Quarterly Journal
Submission and Style Guidelines

Connections accepts manuscripts in the range of 2,000 to 5,000 words, written in a lucid style for a target audience of informed defense and security affairs practitioners and academics. All manuscripts should be submitted to the *Connections* editorial office electronically at PfPCpublications@pfp-consortium.org. They should feature the author's name, current institutional affiliation, and a provisional title at the top of the first page, and should include footnotes where necessary. Additionally, authors should provide a manuscript abstract and keywords.

Preferred themes for journal future editions include:

Arctic Exploitation and Security
Arms Control and European Rearmament
Challenges and Opportunities in Intelligence Sharing
Countering and Preventing Violent Extremism
Cybersecurity
Defense Institution Building
Future Security Scenarios
Hybrid Warfare
Limitations of Naval Power
Migration and Refugees
NATO's Unstable Periphery
Putin's Russia: A Threat to Peace or a Threat to Itself?
Terrorism and Foreign Fighters
Trends in Organized Crime

For questions on footnotes and references, please refer to the Chicago Manual of Style, at http://www.chicagomanualofstyle.org/tools_citationguide.html.

Unsolicited manuscripts are accepted on a rolling basis at the discretion of the PfPC Editorial Board.

The theory of deterrence emerged with the advent of nuclear weapons to address the challenges of preparing for and preventing a full-scale nuclear war between the United States and the Soviet Union. The contributions to this special issue are set in a post-Cold war context, with a resurgent and aggressive Russia. The set of articles provides an outline of the theory of deterrence, the current practice of its application in deterring and, if necessary, defending by conventional forces NATO and Europe's Eastern flank against aggression, and critical analysis of its pertinence to cyber and hybrid warfare.

For all information regarding
CONNECTIONS, please contact:

Partnership for Peace - Consortium
Managing Editor
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2256
E-Mail: PfPCStratCom@marshallcenter.org

ISSN 1812-1098
e-ISSN 1812-2973