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).

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.

Acknowledgment

Connections: The Quarterly Journal, Vol. 18, 2019 is supported by the United States government.

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/.