Information & Security: An International Journal

Todor Tagarev, v.39:3, 2018, 289-300 https://doi.org/10.11610/isij.3924

HYBRID WARFARE: EMERGING RESEARCH TOPICS

Todor TAGAREV

Abstract: This article elaborates on four emerging research topics, considered of key importance for the understanding of and finding effective countermeasures to hybrid threats: (1) exploring the interlinked dynamics of a conflict developing in parallel in the physical world and on social networks; (2) analysing the expanding involvement of private actors who serve as proxies for an assertive state; (3) exploring the vulnerabilities of national security systems to hybrid influence and finding effective countermeasures; and (4) designing an architecture that allows to study the problem of hybrid threats holistically by providing interoperability among domain-specific or cross-domain models, or 'use cases,' and the respective data. All these require multi- and interdisciplinary research and consistent accumulation, verification and sharing of data, case studies and models.

Keywords: hybrid warfare, hybrid threats, vulnerability, risk, complexity, nonlinearity, multidisciplinary studies, interdisciplinary research.

Introduction

> *The most powerful enemy can be vanquished only by exerting the utmost effort, and by the most thorough, careful, attentive, skilful, and obligatory use of any, even the smallest, rift between the enemies, any conflict of interests among the bourgeoisie of the various countries and among the various groups or types of bourgeoisie within the various countries and also by taking advantage of any, even the smallest, opportunity of winning a mass ally, even though this ally is temporary, vacillating, unstable, unreliable, and conditional.*
>
> – Vladimir Lenin [1]

Throughout human history, conflicts and wars have been waged with very little restraint either on legal or on moral grounds. Usually, opposing parties have used all

means at their disposal to overcome the will of the opponent. Conflicts in the Twenty First Century make no exception in that regard. Rather, the free movement of people, goods and capital, liberal norms of ownership and operation of assets, including by foreign entities, new technologies, and in particular the easy access to technologies for networking and instant communication provide ample opportunities to add new tools to the already rich warfare toolbox.

After the 2006 Lebanon war, analysts introduced the term 'hybrid warfare' to reflect better the expanding variety of tools used in conflict. Analysis has demonstrated that a dedicated opponent, who may be disadvantaged militarily and economically, but follows consistently Lenin's advice and is open to innovation, can still achieve his political objectives or, as a minimum, poses considerable challenges.

Since the spring of 2014, when Russia grabbed a territory of 27 thousand square kilometres—roughly the size of the state of Massachusetts—without having to fight a war against Ukraine, the concept of hybrid warfare became a subject of intensive studies and widest interpretations. Not surprisingly, so far it has not been possible to come to a widely accepted definition of the term. On the contrary, often it is used in discussing scenarios in which the military is not—and is not even expected to get—involved.

Nevertheless, worries are often well justified, and policy makers need to consider actual or potential hybrid threats, to assess vulnerabilities, elaborate and implement measures of protection. The research community responds to the need by developing, as the current volume of "Information & Security: An International Journal" [2] demonstrates, methods and models for analysis of the threats, protection measures, concepts, procedures and organizational arrangements, etc. Most of the respective studies are domain-specific, and the majority address one the following three themes:

1. propaganda, disinformation, e.g. fake news, and the ways they influence the perceptions—and consequently the actions—of decision makers and the population at large;
2. cybersecurity, and the use of cyber space more generally;
3. influence over and the protection of other sectors of critical infrastructure.

This article presents four more specific topics which, in the opinion of the author, are of considerable practical importance and have not yet received due attention by researchers: the mutually reinforcing links between physical conflict and its image on social networks; the use of non-military, non-professional security actors as substitutes in activities which have so far been performed by defence and security personnel; the national security system as a target of hybrid influence; and the need to develop methodological infrastructure to allow appropriate, holistic study of hybrid

threats. The article concludes with a call for wide research collaboration in the accumulation, verification and sharing of data, case studies and models.

Dynamic of Conflict in the Physical World and on Social Networks

> *In the social media age, what you share is deciding what happens on the battlefield*.[3]

The use of social media for the purposes of propaganda, the spread of disinformation, e.g. 'fake news,' in attempts to manage the perceptions of large groups of people, or the "weaponization of social media" more generally, is of continuous interest and has attracted the attention of numerous researchers and policy makers.[4] Social media can, and has already been used [5] to "prepare the battlefield" by shaping the narrative for a targeted audience—both decision makers and the population at large—to achieve a desired effect. It is beyond doubt that future conflicts will be preceded and accompanied by active social media campaigns in which each side will try to manipulate the perceptions of the opposing side, the own population, and the wider international community.

Likewise, an ongoing conflict will be reflected in debates on social networks with contributions by people with high stakes in the outcome of the conflict, at one end, to people that are just curious on the other.

Thus, the first emerging theme, presented here, is the bi-directional link between conflict in the physical world and on social networks. Echoing Trotsky's "You may not be interested in war, but war is interested in you," Peter Singer and Emerson Brooking formulate it in their contribution to the 'Argument' section of *Foreign Policy*.[6]

The authors reconfirm the importance of using social media to own's advantage by quoting General Stanley McChrystal, former commander of Joint Special Operations Command, of the International Security Assistance Force and the U.S. Forces in Afghanistan, stating that "Shaping the perception of which side is right or which side is winning will be more important than actually which side is right or winning." The novelty in their findings that "the messages coursing through social media today shape not just the perceived outcomes of conflicts but the very choices leaders make during both military campaigns." In support to this finding the authors refer to Russia's information operations in Ukraine, as well as the study of Prof. Thomas Zeitzoff of the Israel Defence Forces' 2012 air campaign against Hamas in the Gaza Strip, who has found that "the conflict *followed* the pace set on Twitter; the tempo of operations and targeting shifted depending on which side was dominating the online conversation at the time. The military officers and civilian leaders were watching their social media feed and reacting accordingly."[7]

Singer and Brooking provide recent examples how social media posts have built on existing fault lines, triggering violence in Sri Lanka, India, and Myanmar, as well as making it much more challenging to end a conflict. They also point to two developments—in artificial intelligence and using hyper-realistic digital forgeries, or *deep fakes*—in strengthening the influence of social media on future conflicts.

Hence, the interplay of propaganda and information operations, social media, and artificial intelligence, and the mechanisms of governance of the latter two, is expected to attract the attention of both researchers and policy makers in the years to come, and will require significant interdisciplinary efforts.

Active Measures by Proxies

The term 'hybrid warfare' is relatively new, in use for just over a decade. The concept, however, is as ancient as warfare. Some authors trace the implementation of the concept by Russia as far back as the Eighteenth Century, culminating then in the first annexation of Crimea by the Russian Empire under Empress Catherine the Great, and described in her Manifest of April 19, 1783 addressing the other Great Powers of Europe. In justifying her actions, in the document she claimed that it is necessary "to protect the people there" and described the range of political, diplomatic, legal, cultural, economic and intelligence tools used to annex the peninsula.[8]

In the Soviet times, the concept implementation thrived under the doctrine of "active measures"—an element of "political warfare"—that integrated a broad range of influence activities including, among others, overt propaganda, covert media placement, forgery, agents of influence, 'friendship' societies, front organizations, drug trafficking, incitement, assassinations, illicit support of terrorism.[9]

Nevertheless, in practice, active measures were tightly controlled by the Politburo and the Secretariat of the Communist Party of the Soviet Union, which approved the major themes of respective operations.[10] The measures were implemented by officers of KGB and the military intelligence via covert operations and trying to assure 'plausible deniability' for the involvement of state actors.

These operations were likely decreased in scope and ambition immediately after the end of the Cold war, but not terminated. Novelties in the implementation of the doctrine were introduced in account of the process of globalization and the opportunities it provides for free flow of information, internet-based communications, travel, financial transfers, investments, and cultural exchanges. Specifically for Russia, important changes were introduced as a result of redistribution of wealth after the dissolution of the Soviet Union and the interlocking of political, business power and the power of security players, or the so called '*siloviki*,' that brought under the limelight a number of Kremlin-affiliated oligarchs. That in turn made more prominent the role of private

actors that seem to willingly serve as proxies for the Russian state in exercising hybrid influence.

The role of private military companies in Moscow's strategy of "multi-domain coercion"[11] has been covered to a large extent. Here are some recent cases involving other companies and individuals, that confirm this thesis:

- The coup attempt in Montenegro on the election day in October 2016 with alleged involvement of officers from the Main Intelligence Directorate (GRU) of Russia's defence ministry together with Serbian and Montenegrin citizens, while the Russian tycoon Constantine Malofeev exercised considerable impact though his own TV station in Montenegro and influence over leaders of opposition political parties and senior clergy of the Serbian Orthodox Church;[12] some authors even argue that the plan for the coup originated in conservative nationalist circles surrounding Malofeev.[13]
- Allegations that former Trump election campaign chairman Paul Manafort has received a $ 10 million loan from the Russian oligarch Oleg Deripaska and that, years earlier, Deripaska had paid Manafort for his consulting work for Ukraine's former President Viktor Yanukovych, backed by Kremlin;[14]
- Organization and financing by Russian private actors of paramilitary structures and 'patriotic youth camps,' in particular in Eastern and South-Eastern Europe;[15]
- Financing "sports and (counter)cultural" organizations, such as the "Night Wolves" by "Wolf Holdings," owned by Gennady Nikulov – a former military officer and current vice-president of Sevastopol's pro-Russian "self-defence forces."[16] Using a site owned by an entrepreneur with ties to right-wing Slovak militias, the "Night Wolves" even managed to establish an official base for para-military type of presence in a NATO and EU member country;[17]
- Private acquisition of property of potential strategic importance. For example, Pavel Melnikov, a Russian from St. Petersburg with a number of identities and several passports, has bought an island in an archipelago between Finland and Sweden where he built nine piers, a helipad and enough housing with sophisticate communications "to accommodate a small army."[18]

All these examples indicate the increased geopolitical ambitions of a resurgent Russia and its quick adaptation to—and exploitation of—the opportunities provided by more open, democratic societies. The involvement of private actors as proxies adds another degree of complexity in the study of hybrid threats. One needs to understand not just the ways in which the security apparatus of a country is exercising hybrid influence functions, but also the capacity to reveal and understand the mechanisms of state po-

litical and economic power in a "managed democracy" like Russia's,[19] as well as the vulnerabilities in democratic societies facilitated by the free flow of money and assets. This combination frames the second emerging topic in the study of hybrid warfare.

Are the Guardians Immune to Hybrid Threats

The third emerging topic addresses the vulnerabilities of the security apparatus and the ways in which these vulnerabilities can be—and already are—exploited by an adversary. The majority of analysts tend to examine the problem of hybrid threats in a dichotomy – there are parts of state and society that are vulnerable and need to be protected, and then there is the security sector to protect and defend against hybrid influence (among other threats) in the most effective and efficient manner. But is this really the case?

The developments in Ukraine in the spring of 2014 painfully demonstrated that a corrupt and inefficient security sector is an easy prey of manipulation, and even people at highest leadership positions can turn to be valuable assets in the hands of the enemy. Thus, at the end of February 2014, the defence minister Pavlo Lebedev fled Ukraine with ex-President Viktor Yanukovych 2014 amid the EuroMaidan Revolution,[20] and later the same year ran for a seat in the city council on Sevastopol in the Russia-annexed Crimean Peninsula.

In regard to the armed forces, at the time of the Maidan, the Ukrainian military had limited training and a variety of problems with logistics. And yet, between 15,000 and 18,800 Ukrainian troops were stationed in Crimea towards the end of February 2014, plus another 2,500 troops of the Ministry of the Interior. Russian troops stationed in Crimea numbered approximately 12,000, with only one brigade of marines, and in total were inferior to the Ukrainian military in terms of firepower.[21]

Irrespective of what the actual capability of Ukrainian military forces in Crimea was, they could have put a fight and dissuade Kremlin from sending more "polite green men" to the peninsula. But they did not. Here are two examples on the side of the senior military. First, rear admiral Denis Berezovsky, who was appointed commander-in-chief of the Ukrainian Navy on March 1, 2014, defected on the following day along with several of his commanders,[22] and on March 24, 2014 was appointed deputy commander of the Russian Black Sea Fleet by the defence minister of Russia Sergei Shoigu. Likewise, Sergei Yeliseyev, first deputy commander of the Ukrainian fleet in 2014, did not resist but instead quit, and was later assigned as deputy chief of Russia's Baltic Fleet.[23] Others stayed, but did not resist and surrendered Crimea.

Russia attempts to create exploitable vulnerabilities in security and defence sectors of other countries as well, including members of NATO and the European Union. Mihail Naydenov identifies several ways used for that purpose:[24]

- indirectly, through manipulation of the public opinion and fuelling division on NATO membership;
- supporting euro-sceptic, anti-Western, pseudo-nationalist and pro-Russian politicians and parties which, especially when in power, encourage respective sentiments among security and defence personnel;
- nurturing nostalgia, particularly amongst retired military personnel and associations of reservists;
- supporting the contribution to NATO and the EU common security and defence policy in words, while in practice maintaining legacy equipment, concepts and methods, and hindering defence modernisation and interoperability;
- mismanagement and corruption.

Pursuing the same objective, Todor Tagarev suggests an analysis framework based on a simplification of John Warden's "five rings model" (briefly addressed in the next section) and highlights the following venues of hybrid influence:[25]

- influence over the personnel via general purpose propaganda, propaganda tailored to security sector organizations, specialised publications and organizations of reservists and retired personnel, the 'revolving door' policy, direct influence over paramilitary organizations and private companies of relevant scope of activity;
- influence over the defence and security 'infrastructure' – repairs and maintenance of main combat and supporting equipment, defence industrial companies, other suppliers of specialised equipment and services;
- critical resources – influence over the budgeting process (e.g. by consistent underfunding of defence), research and technology development, education, etc.
- direct influence on the leadership with promises for a political or a business career, creating opportunities for coercion based on prior involvement in corruption or other dependencies, participation in 'secret societies,' etc.

The understanding of this emerging theme, which goes way beyond the traditional recruitment of human agents, or spies, requires interdisciplinary research combining system analysis, anthropological studies, and understanding of contemporary theories and policies of governance and integrity in defence in security, as well as consistent accumulation and sharing of data and cases studies.

Applicability of Risk-oriented Decision Frameworks

Main purpose of rigorous analysis is to assist the formulation and implementation of sound policies, in the case of interest – policies for countering hybrid threats. A proven framework is that of risk management, codified for example in the ISO 31 000 series of standards. In the face of an intelligent opponent, risk management requires understanding of our own vulnerabilities, as well as the capability and the intent of the opponent.

In its hybrid warfare project, the "Multinational Capability Development Campaign" suggests an analytical risk-based framework that builds on three discrete, but interlocked, categories:

- critical functions and vulnerabilities of the defender;
- attacker's synchronized use of multiple means and exploitation of horizontal escalation; and
- linear and non-linear effects of a hybrid warfare attack.[26]

Another framework under consideration builds on Colonel John Warden's "Five Rings model," developed initially for the purposes of air campaign planning.[27] The model presents the enemy's 'system' in five concentric rings representing respectively (from the centre outwards) leadership, system essentials, infrastructure, population, and fielded military. Warden studies each of the rings as a number of nested models of the same kind with account for the linkages among rings and sub-rings. The purpose of the analysis is to find those vulnerabilities in the enemy's system, or 'centres of gravity,' which—when attacked with precision—will lead to its strategic paralysis.

Recently, Nebojsa Nikolic has suggested to connect Warden's rings and hybrid warfare's modes of operation in a matrix analysis and provided an illustrative example.[28] Unlike the original implementation, the purpose here is to identify key vulnerabilities of our own 'system' to the envisioned variety of hybrid tools, as well as opportunities to invest in and the utility of respective measures for protection.

Analysts using both frameworks build on heuristic models and, so far, have been able to provide illustrative cases and examples of better visualisation. This is not surprising, given that available data is not sufficient to construct a model properly reflecting the complexity and intrinsic nonlinearities of hybrid warfare.

In the face of an opponent, willing to use practically *any* tool at its disposal—diplomacy, propaganda, disinformation, inciting riots, cyberattacks, attacks on public services, the energy, transport and financial infrastructures, and even the private life of persons of potential interest,[29] all that along the military instruments—one needs to apply a '*whole of society*' approach to understand own vulnerabilities and how they

can be protected. Creating models of such size and complexity seems to be beyond the capacity of even best resourced organizations, e.g. the intelligence agencies of most powerful countries in the world.

Hence, the fourth emerging topic of hybrid warfare research is the development of comprehensive architecture or a framework, that provides methodological guidance and guarantees interoperability of models and data, while developing domain specific or cross-domain 'use cases' to represent hybrid attacks and protective measures that are based on real world data and evidence, and which can be replicated and independently validated.

One such model attempts to represent the influence of Russia in the energy sector of five countries in Central and Eastern Europe and, based on the accumulated data, demonstrates how "Russia has cultivated an opaque network of patronage across the region that it uses to influence and direct decision-making" and how in an "unvirtuous circle" the political or economic penetration Russia seeks "to gain influence over (if not control of) critical state institutions, bodies, and the economy and uses this influence to shape national policies and decisions."[30]

Conclusion

Even though it has a new name, hybrid warfare is not a novel concept. The term got traction after the 2006 Lebanon war, known also as 2006 Israel-Hezbollah War, and saw widespread and intensive use after the Russian annexation of Crimea. Hundreds, possibly thousands of publications in scientific and professional journals analyse the concept and its various manifestations, and suggest measures to counter hybrid threats. This volume does not make an exception by addressing threat vectors, conceptual, doctrinal and legal foundations for countering hybrid threats, interagency and international cooperation, technologies, analytical support, education and training, and the importance of building organizational and societal resilience. Most of the respective studies are interdisciplinary in nature and build, at best, only on partial evidence.

This article presents four hybrid warfare related topics that have been barely addressed while, in the opinion of the author, require significant research effort to provide critically important understanding of the threat and assist policy makers in finding appropriate solutions. The focus, and the majority of the referenced examples are on Russia, but the exploration of these themes would be beneficial for understanding other actors as well.

As a rule, the effective handling of the topic of hybrid warfare requires multidisciplinary and interdisciplinary studies, scrupulous accumulation, verification and sharing of data, case studies and models. Towards that purpose, the community of likeminded

professionals may benefit from common, open access repositories and the power of social networks,[31] exploit synergies and increase efficiencies for the common good.

Notes

1 Reference to United States Information Agency, *Soviet Active Measures in the "Post-Cold War" Era* (Washington, D.C., 1992), as quoted in Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal* 15, no. 1 (2016): 5-31, https://doi.org/10.11610/Connections.15.1.01.

2 *Interagency and International Cooperation in Countering Hybrid Threats*, edited by Yantsislav Yanakiev, vol. 39 (2018) of *Information & Security: An International Journal*, https://doi.org/10.11610/isij.v39.

3 Peter W. Singer and Emerson Brooking, "The Future of War Will Be 'Liked'," *Foreign Policy*, October 2, 2018, https://foreignpolicy.com/2018/10/02/future-of-war-memes, accessed October 25, 2018.

4 See, for example, Anna Reynolds, ed., *Social Media as a Tool of Hybrid Warfare* (Riga: NATO Strategic Communications Centre of Excellence, May 2016), www.stratcomcoe.org/social-media-tool-hybrid-warfare, accessed October 20, 2018; and Georgii Pocheptsov, "The Fakes in Social Media: Design, Transformation, Insertion in Mass Consciousness," *Rostov Electronic Gazette* 17(350), November 1, 2018 (in Russian), www.relga.ru/Environ/WebObjects/tgu-www.woa/wa/Main?textid=5635.

5 "During the 2014 annexation of Crimea, the Russian government spent more than $19 million to fund 600 people to constantly comment on news articles, write blogs, and operate throughout social media." – as cited in Michael Holloway, "How Russia Weaponized Social Media in Crimea," *RealClear Defense*, May 10, 2017, with reference to Patrick Duggan, "Harnessing Cyber-technology's Human Potential," *Special Warfare* 28, no.4 (October-December 2015), 15.

6 Singer and Brooking, "The Future of War Will Be 'Liked'."

7 Singer and Brooking, "The Future of War Will Be 'Liked'."

8 Georgi Beltadze interviewing Mark Voyger, "Mark Voyger: Russian Hybrid Warfare Can Still Bring Surprises in the Future," *Postimees*, June 18, 2018, https://news.postimees.ee/4505726/mark-voyger-russian-hybrid-warfare-can-still-bring-surprises-in-the-future.

9 Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia." See also "KGB Training Manuals Revealed," *The Interpreter*, November 1, 2018, with links to eight recently declassified KGB manuals, in Russian, and a synopsis of each one in English, http://www.interpretermag.com/kgb-training-manuals-revealed.

10 Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," 11.

11 The formulation of the "multi-domain coercion" strategy is attributed to the Israeli scholar Dmitry Adamsky. See Stephen Blank, "The Role of Private Military Companies in Russian National Security Strategy," Defense.Info, August 3, 2018, https://defense.info/dannys-corner/2018/08/the-role-of-private-military-companies-in-russian-national-security-strategy/.

12 Ivana Gardasevic, "Russia and Montenegro: How and Why a Centuries' Old Relationship Ruptured." *Connections: The Quarterly Journal* 17, no. 1 (2018): 61-75.

[13] Dimitar Bechev, "The 2016 Coup Attempt in Montenegro: Is Russia's Balkans Footprint Expanding?" Russia Foreign Policy Papers (Philadelphia, PA: Foreign Policy Research Institute, April 2018), https://www.fpri.org/article/2018/04/the-2016-coup-attempt-in-montenegro-is-russias-balkans-footprint-expanding.

[14] Cristina Maza, "Paul Manafort's Ties to Russian Oligarch Run Deeper than Expected, Investigation Reveals," *Newsweek*, June 28, 2018, https://www.newsweek.com/paul-manaforts-ties-russian-oligarch-run-deeper-expected-investigation-reveals-999854.

[15] Sergey Sukhankin, "Russian PMCs, War Veterans Running 'Patriotic' Youth Camps in the Balkans," *Eurasia Daily Monitor*, Part One v. 15 (151), October 24, 2018, https://jamestown.org/program/russian-pmcs-war-veterans-running-patriotic-youth-camps-in-the-balkans-part-one; and Part Two by the same author, v. 15 (155), October 31, 2018, https://jamestown.org/program/russian-pmcs-war-veterans-running-patriotic-youth-camps-in-the-balkans-part-two/.

[16] Mitchell A. Orenstein and Peter Kreko, "How Putin's Favorite Biker Gang Infiltrated NATO," *Foreign Affairs*, October 15, 2018, https://www.foreignaffairs.com/articles/russian-federation/2018-10-15/how-putins-favorite-biker-gang-infiltrated-nato.

[17] Orenstein and Kreko, "How Putin's Favorite Biker Gang Infiltrated NATO."

[18] Andrew Higgins, "Finnish Soldiers find 'Secret Russian Military Bases' after Raiding Mysterious Island," *Independent*, November 1, 2018, https://www.independent.co.uk/news/world/europe/finland-russia-military-bases-sakkiluoto-putin-dmitry-medvedev-police-a8612161.html.

[19] See, for example, David Mandel, "'Managed Democracy': Capital and State in Russia," *Debatte: Journal of Contemporary Central and Eastern Europe* 13, no. 2 (2005): 117-136; and Daniel Beer, "Russia's Managed Democracy," *History Today* 59, no. 5 (May 2009), https://www.historytoday.com/daniel-beer/russias-managed-democracy.

[20] Natalie Vikhrov, "Fugitive ex-Defense Minister Continues to Battle EBRD," *Kyiv Post*, March 24, 2017, https://www.kyivpost.com/business/fugitive-ex-defense-minister-continues-battle-ebrd-bank-says.html.

[21] Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: Rand, 2017), www.rand.org/pubs/research_reports/RR1498.html.

[22] "New Head of Ukraine's Navy Defects in Crimea," *BBC News*, March 2, 2014, https://www.bbc.com/news/world-europe-26410431.

[23] Pavel Polityuk and Anton Zverev, "Why Ukrainian Forces Gave up Crimea Without a Fight – and NATO is Alert," *Reuters*, July 24, 2017, https://www.reuters.com/article/us-ukraine-crisis-crimea-annexation/why-ukrainian-forces-gave-up-crimea-without-a-fight-and-nato-is-alert-idUSKBN1A90G0.

[24] Mihail Naydenov, "The Subversion of the Bulgarian Defence System – the Russian Way," *Defense & Security Analysis* 34, no. 1 (2018): 93-112.

[25] Todor Tagarev, "Main Avenues for Hybrid Influence over the National Security System," in *Proceedings of the Conference "Hybrid Threats: Myth or Reality? Consequences for the National and the European Security,"* Sofia, Sofia University "St. Kliment Ohridski," 16-17 October 2018 (under print).

[26] Patrick J. Cullen and Erik Reichborn-Kjennerud, *Understanding Hybrid Warfare* (Multinational Capability Development Campaign – Countering Hybrid Warfare Project,

January 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf, accessed November 5, 2018.

[27] John Warden, *The Air Campaign: Planning for Combat* (Washington, DC: Pergamon-Brassey's, 1989).

[28] Nebojsa Nikolic, "Connecting Conflict Concepts: Hybrid Warfare and Warden's Rings," *Information & Security: An International Journal* 41 (2018): 21-34.

[29] "Russian woman charged with spying in the US," *BBC News*, July 16, 2018, https://www.bbc.com/news/world-us-canada-44854365.

[30] Heather A. Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, D.C.: Center for Strategic and International Studies and Rowman & Littlefield, 2016), p. xii, https://www.csis.org/analysis/kremlin-playbook.

[31] One example in this respect is "The Hybrid War" group on Facebook, https://www.facebook.com/groups/1615853818647978/.

About the Author

Prof. Todor Tagarev is Head of the Centre for Security and Defence Management, Institute of ICT, Bulgarian academy of Sciences, Co-President of the Atlantic Council of Bulgaria, and member of European Leadership Network. He has held variety of senior civilian positions in Bulgaria's Ministry of Defence and served as defence minister in Bulgaria's Caretaker Government, March – May 2013.