Information & Security

Raychev, vol. 43, no. 3 (2019): 349-361
https://doi.org/10.11610/isij.4326

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Cyberwar in Russian and US Military-Political Thought: A Comparative View

Yavor Raychev

University of Granada, Granada, Spain, https://www.ugr.es/

ABSTRACT:

In this paper I argue that there are huge differences in the concepts of cyberwar in Russian and American politico-military thought. Cyberwar is a part of modern hybrid war. In the American views, the latter was coined to describe certain new forms of warfare, above all in the Middle East. It is based on analysis of the experience of various terrorist and jihadist groupings acting in the area. In the Russian tradition, before the disintegration of USSR "hybrid war" (although different terms were used) referred rather to political and information operations. In this century, the Russian concept was developed in a close relation with coloured revolutions, the Arab spring, the Russian intervention in Ukraine and the perception that the country is permanently attacked by the US and their Euro-Atlantic allies. Here, the Russian and the US concepts are compared by origin, conceptual basis, scope, nature, time to be waged, tools, relations with other fields, how are they organized and who are the cyber actors. Fundamental differences are established, and this is one of the reasons for certain ineffectiveness of the West in meeting the challenges of modern Russian hybrid war in general and cyberwar in particular.

ARTICLE INFO:

RECEIVED: 10 MAY 2019
REVISED: 10 SEP 2019
ONLINE: 22 SEP 2019

KEYWORDS:

cyber war, hybrid warfare, Russia-NATO relations

Introduction

One of the frequently asked questions in the field of international security is why EU and NATO, which dispose of much more resources that Russia, and technically are much more advanced, are not able to successfully meet Russian hybrid challenges, part of which is cyberwar. The short answer is: because West-

✉ Tel.: +359886109876; E-mail: yavorraychev1988@gmail.com

erners just do not understand what Russians do mean. The long one – that Russia has an immense experience in waging hybrid war and special operations against its enemies and because among all great powers today, it has the longest experience in the field of cyber war. As a result, Russia has learned to be the perfect opportunist in the international system. The lack of understanding of the "Russian" way of conducting hybrid war and, especially, of using one of its tools – cyberwar, is and will potentially be weakening the ability of the NATO members to adequately meet this challenge.

Methods

In this article I argue that Russian and US concepts of cyberwar as one of the tools of hybrid war strongly differ because they are fruit of different historical experience, political and strategic culture. The lack of understanding of the "Russian way" to wage cyberwar is and will potentially be weakening the ability of the NATO members to adequately meet this challenge.

The main method to be used is the comparative analysis. At the beginning I describe the Western and Russian concept of cyberwar. Afterwards, I compare Western and Russian concepts following the next criteria: origin, conceptual basis, scope, nature, time to be waged, tools, relations with other fields, ways of organization, participants. Then I use a case study in order to illustrate differences. Finally, I draw the conclusion that the vulnerability of Western states and societies is due to the fact that they do not understand the nature of the real threats to national and international security.

It needs to be clearly said that the current article is not concentrated on the technical aspects of cyberwar; it is about the role of technology, and especially, of high tech in foreign policy. Besides, it does not seem that hybrid war is a direct consequence of the revolution in IT sector; it has rather to do with their social implications.

Western Views about Cyberwar

Cyber warfare is often seen as another transformation in military affairs; one of several that took place under the impact of technologies and their implementation in different countries and epochs. Sometimes these changes are so deep that they are changing the whole concept of war: our understanding about offensive and defensive operations, just and unjust war, etc. "Cyber-warfare involves multiple units (individual, state-sponsored organizations, or even nations) executing simultaneously offensive and defensive operations through networks of computers."[1] It is directed against people, machines, and infrastructure and is not question of the future; it is reality here and now[2] and, as such, should be examined as an immediate challenge to national and international security.

In some way, cyberwar is a consequence of cyber dominance of the West; a dominance that helped it win the Cold war. However, today developed countries are totally dependent on the technologies, and technologies are already available to their competitors, rivals and enemies. To wage a cyberattack is

much cheaper that to wage any other attack; then, the temptation to use it is really great for states, armies, corporations and hacktivist groups.

Before defining cyberwar, a definition of "cyber" is needed. The definition of UN states the next: cyberspace is "The global system of systems of internetted computers, communications infrastructures, online conferencing entities, databases, and information utilities generally known as the Net. This mostly means the Internet; but the term may also be used to refer to the specific, bounded electronic information environment of a corporation or of a military, government, or other organization."[3]

Cyberwar is viewed by Western scholars as a specific form of cyber conflict. There are many classifications of the latter. Jajodia et al., for instance, speak about four types: "(1) social media wars that influences a country's internal politics often with a goal of fomenting social uprisings that can result in political change; (2) strategic war aimed at causing damage for the adversary as well as pillaging resources (e.g., industrial espionage); (3) ideological battle where fundamentalist organizations use the Internet to spew their ideology and to recruit members in other countries for their cause; (4) citizen-initiated war where a country's civilians directly attack another country's citizens and institutions as a part of larger conflict (ideological or kinetic)."[4]

Cyberwar shares elements with all the kinds of cyber conflicts, but is not reduced to any of them. Then, what is cyberwar? The Western concept of cyberwar can be tracked back to Arquilla and Ronfeldt who already in 1993 distinguished between two terms "netwar" – societal-level ideational conflicts waged in part through internetted modes of communication, and "cyberwar" at the military level. Both share some common features: they revolve around information and communication matters, what means that at a deeper level they are forms of war about "knowledge" – "about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries."[5] Some scholars use "information war" and "cyberwar" as synonymous, while others reject such a use. Mehan argues that information war (IW) is much broader concept that includes any technique to disrupt or affect an entity's information use – cyberattack, electronic warfare, psychological operations, or intentional deception. By using the terms interchangeably, IW is inadvertently tied to cyber warfare even though it has a much broader mandate. In her next book, Mehan refines her view as follows: "Cyberwarfare, thus, infers both an information-related conflict at the national, military level, as well as low intensity conflict activities intended to inflict limited levels of damage."[6]

The European Security and Defence Assembly (1954-2011) interpreted "cyberwar" as "digital war," as a capacity to lead a war in cyberspace through computers and internet. The US Department of Defense identifies cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the In-

ternet, telecommunications networks, computer systems, and embedded processors and controllers" – a definition adopted also by the National Institute of Standards and Technology.[7]

As it can be seen, since the very beginning, definitions concentrate exclusively on military aspects – technical, strategic, organizational, and doctrinal. Technical aspects have to do with how to prepare and conduct military operations; disrupting and destroying information and communication systems; military culture, understood as knowledge of itself (capabilities, ways of acting, etc.). They are also related to the technologies: intelligence collection, processing, and distribution; tactical communications, positioning, and "smart" weapons systems; electronically blinding, jamming, deceiving, overloading, and intruding into an adversary's information and communications circuits.[8] It should be recognized that Arquilla and Ronfeldt call the attention to the fact that cyberwar "is not simply a set of measures based on technology"; that it calls for "new approaches to plans and strategies, and new forms of doctrine and organization." However, in their elaborations, they never went beyond military matters and aspects.

This trend proved to be durable in Western political and military thought. Almost 20 years later Western experts continue to be of the same opinion: "As long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk."[9] Following the same technocratic logic, Libicki offers more nuanced understanding of cyberwar; he distinguishes between operational cyberwar,[10] understood as acting against military targets during the war; and strategic cyberwar – cyberattacks on enemy civilian structures [11] and/or "a campaign of cyberattacks launched by one entity against a state and its society, primarily but not exclusively for the purpose of affecting the target state's behavior."[12]

Then, how the cyberwar looks like? In 2009, the cyberwar was defined in the following way: "Typical cyber warfare tactics include website defacement; denial of service attacks; domain name service attacks; use of worms, viruses and Trojan horses; exploitation of inherent computer security loopholes and unauthorized intrusions into an opponent's computer systems and networks. Defacement means the disruption of a website so that it no longer performs the function for which it was designed. It usually includes altering the contents of the page by placing on it, for example, propaganda, profanity or pornographic images. Domain name service attacks aim to secretly redirect traffic from one website to another, usually to one on the attacker's own server. It enables the attacker to disseminate false information and mislead web users."[13] The primary purpose would be to enhance the effect of physical attack. Today we know that cyberwar might lead to sabotage in nuclear facilities, disturbance in the power supply and the electric grid of the city, sabotage bank systems and media.

Some analysts divide cyberwar in classes. Class I cyberwar is concerned with the protection of personal information – or personal privacy. Class II cyberwar

concerns itself with industrial and economic espionage, which can be directed against nations, corporations, universities, or other organizational structures. Class III cyberwar is about global war and terrorism. Finally, Class IV cyberwar is the use of all of the techniques of Classes I – III in combination with military activities in an effort to obtain a battlefield advantage or a force multiplier.[14]

Ventre is one of the very few Western authors who went beyond this technocratic concept – he spoke about cyberwar as a war of meaning, based on the values which underline the ideologies of belligerent parties. Neither computers, nor internet do the war; it stems from different ideologies that could led people to situation of confrontation, including to a war.[15]

It can be concluded that Western view on cyberwar is predominantly military-focused and technocratic. It views cyberwar in the broader context of cyber conflict as a modern form of fighting, but hardly grasps its social dimensions. Developed initially by two scholars, one of them closely related to the US military, it was born as confined to military affairs. Moreover, in the Western concept, cyberwar is viewed as a separate domain, distinct from information warfare and its associated psychological aspects. Despite certain nuances, in the next 20 years it remained basically unchangeable, with very few intentions to be broadened. Neither attacks against Estonia, nor the Georgia war were able to transform the Western concept and to turn Western scholars towards a wider understanding of cyberwar.

The Russian-Ukrainian crisis and illegal annexation of Crimea made various scholars re-think their positions. After 2014, we witnessed an increasing understanding that Russia is guided by other rules; and these rules are no longer about computers, ports and protocols, but about the way Russians manipulate social media in order to convert them in a perfect hacking tool, about networks of professional troll factories and about the fact that all they are coordinated by Russian security services in a unique military campaign, waged mainly by non-kinetic means.

Just because of lack of understanding of Russian concept, the Russian cyberwar is that successful. In 2016, John McCain recognized their lead and concluded that "they [Russians] are in many ways ahead of us in all this cyberwar. We need to solve this whole problem of cyberwar, in which we have neither strategy nor politics. This is one of the areas in which they have an advantage, probably the only area in which our opponents have an advantage over us."[16]

The Russian View

Russian cyberattacks against West are not new; they date at least since 1986, when Soviet cyber operators worked in a close cooperation with secret services of the German Democratic Republic in order to damage West German cyber proxies.[17] During the crisis of the 1990s, with its economic difficulties, the trend to develop cheap, but effective military strategies continued. Russia's investment in cyber capabilities increased in the 2000s, when it had to meet the challenge of the information campaign of Chechen rebels and later having to neu-

tralize weak, but noisy opposition groups which fought for place in Russian political life. Internet became a battlefield also between Putin and independent media, which were soon silenced with cyber means. Since then Russia, without being the only source of cyber threats (North Korea, Iran, China also source malicious cyber actors), is an example of a great power that successfully integrates cyberwar in its foreign policy and relationship with adversaries and allies. The conceptual basis of all this become the Information Security Doctrine, signed by Putin in 2000, and covering a wide spectrum of issues, staring with spiritual security, passing through cybersecurity and ending with information security.[18] The new doctrine follows the same path; also in it, in the section "Strategic aims and main areas of information security," social effects of what a Western expert would call "cyberwar" are mentioned before technical ones.[19]

A more detailed view on Russia military thought will show that "Russia has integrated cyber and information warfare organically into its planning and capabilities to project power." It has converted cyberattacks in "an organic element of a long-standing approach to political war-fare and information operations." Cyberwar and information war are seen by Russian militaries as two inseparable components of information confrontation (Informatsionoye protivoborstvo) "and are to be fully integrated in any campaign with military operations." Then "in Russian discussions and practice, distinguishing cyber war from IO is virtually impossible."[20]

This does not mean that Russia is not prepared to attack through internet key military and civilian facilities and infrastructures. The US director of National Intelligence Gen. James Clapper testified in 2015 that Russia has such capabilities[21] – this is proved by Russian attacks against Ukrainian electricity sector. Probably Russian cyber actors are in the process of developing means for remote control on industrial systems: electric power grids, urban mass transit systems, air traffic control, and oil and gas distribution networks. However, the main efforts of Russia, embodied in the recently settled cyber command,[22] are channelled in another direction.

Russian understanding of cyber operations is closely related to the Soviet concept about political warfare. One of characteristics of Russian political and strategic culture is the perception to live in siege, under attacks of the international capitalism and imperialism, led by USA, whose only idea is to abolish the first state where the dictatorship of proletariat has been established. Despite the fact that nowadays ideology is removed from Russian strategic thinking, it still does not distinguish between peace and war as America does. À la guerre comme à la guerre – if we are in a war, we should prepare every day for the military actions of the enemy in order to enhance our security. In the documents of Russian government since 2009, plans for mobilization of all resources of the country for winning in this permanent conflict can be seen. Most of them are not military, but psychological and informational.

The term cyberwar is rarely used by Russian scholars except in cases when they speak about someone else's cyberattacks against Russia. Just one example from Pravda.ru news website: On October, 14, 2018, the minister of the defence

of The Netherlands, Ms Ank Beyleveld declared that her country is in a cyberwar with Russia. The website in question reacted with an article under the title "People in Russia are amazed that they are in cyberwar with Holland." The same is the case with another journalist's material, published under the title "UK prepares a large scale cyberattack against Russia."[23] Russian political and military analysts prefer to conceptualize cyberwar within a broader field of information war – "a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations."[24]

One more distinctive feature of Russian concept should be considered. The Military Doctrine of the Russian Federation (2010) underlines "the prior implementation of measures of information warfare" in order to achieve political goals without military means."[25] This legitimizes the use of military action in war and peace time, and at the same time "cyber IO affords the Russian government covert means to achieve these objectives, allowing Russia to maintain a degree of plausible deniability with regard to its participation in disinformation campaigns."[26]

How Russian cyberwar is organized? Efforts in this direction started after the Russia-Georgia war (2008) when, despite the victory, some important deficits in information operations were revealed. In order to overcome them, the Ministry of Defence announced the creation of units responsible for such operations, composed by "hackers, journalists, specialists in strategic communications and psychological operations, and, crucially, linguists to overcome Russia's now perceived language capability deficit. This combination of skills would enable the Information Troops to engage with target audiences on a broad front, since for information warfare objectives the use of "mass information armies" conducting a direct dialogue with people on the internet is more effective than a "mediated" dialogue between the leaders of states and the peoples of the world."[27] The idea was amended in 2013 with the decision to create a cyber unit in the army in charge of offensive and defensive cyber operations, cyber research and the functioning of an agency, called the Foundation for Advanced Military Research.

Beside military, other cyber operators appeared as participants in Russian cyberwar. The new tactics of official Russian authorities was to outsource cyber war to informal groups of IT experts – activists, criminal groups, legitimate cyber tech firms, groups of hackers, often called hacktivists, and an "army of trolls." The role and functions of the latter are reviewed in the following case study.

Case Study: Internet Research Agency (IRA)

This case study illustrates what has already be said: information operations are inherent part of Russian cyberwar because they are waged in the global cyber space. It is about so-called Internet Research Agency (IRA), engaged in the scandal of 2016 USA presidential elections.

The first data in the Russian press about the availability of groups of trolls in Petersburg and Moscow, which work on order to influence public opinion, ap-

peared in 2013. A journalistic investigation by Novaya Gazeta alleged that already in August of that year, there were recruitment announcements.[28] The largest organization in the holding was the Federal News Agency, which has at least 16 information sites, nine of which are officially registered as mass media.[29] According to US Deputy Prosecutor Rod Rosenstein, the agency is a structured organization that has a multi-million dollar budget, hundreds of employees and many "shell" companies through which it operates. Again, according to the same source, the organization has graphic and financial departments as well as departments for research and information optimization.

On February 16, 2018, the US Ministry of Justice indicted 13 Russian citizens and three companies for interference in the presidential election in 2016. It emphasized that the interference in the presidential election is part of a larger operation – Project Lahta, which is not limited to the United States. They were charged for eight cases: the first is a conspiracy for fraud against individuals and organizations and the second one – a "conspiracy of mischief" against some officials and the agency as a whole. This group opened accounts with US banks using the personal data of real Americans without their consent (using birth date, address, and insurance number) and used them to transfer money between Russia and US.

In October 2016, the United States officially blamed Russia for interference in the country's elections. In the "Joint Statement of the Department of Homeland Security and the Office of the Director of National Intelligence on Election," it was said:

> The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.[30]

Russia trolls created accounts of fictional people on social networks, turning them into leaders of public opinion in the United States. They entered in contact with real Americans and ran in different cities campaigns in support of both Donald Trump and Hillary Clinton. The task was to shape the agenda of American voters, to influence their opinion, to involve them in discussion. For this, high professional qualities were needed:

> Primitive arguments were not accepted. That's why we needed a deep knowledge of many typical for the life in USA issues – taxes, gay, sexual minorities, weapons. .... They [the supervisors] give you a list of media you need to comment on and which you should monitor. New York Times, Washington Post – there are hundreds of thousands of posts. You must review everything

> and understand the general tendency, what people argue about. And then you have to enter a dispute trying to "shake the boat." For Russia you shouldn't talk at all. Neither Russia nor Putin should be mentioned. Because Americans do not talk about it. They don't care about Russia and Putin… We did not aim to turn the Americans against Russia. We aimed to turn them against their own government. To cause disorder, discontent, to lower Obama's rating. When elections began, we got instructions about who is the better president for Russia, and who should be avoided.[31]

According to the US Justice Department, the agency's main goal is "creating disagreement in the US and undermining public confidence in democracy." Influence is achieved through social media, but without revealing the real nationality of the perpetrators. For this purpose, US IPs are used and VPNs are created.

Russians register hundreds of accounts on Facebook, Twitter and Instagram, using stolen or forged US documents or fictitious bank accounts. They position themselves as "politically and socially active Americans," create network groups, buy advertising, recruit real Americans and pay them to participate in political campaigns and other related activities.[32] These Americans did not realize that they are actually communicating with Russian citizens. On behalf of these Americans, Russians write posts on economic and foreign political issues concerning the United States. The work was done in two shifts to post everything in time, according to the time zone. The calendar of American holidays is used to write up-to-date texts. Activist groups were created in Facebook, Instagram and other social networks for migration, such as Secured Borders; for minorities rights – Black Lives Matter (Blacktivist), United Muslims of America, Army of Jesus; and for regional activism – e.g. South of Heart of Texas.

By 2016, several groups created by the agency had dozens of members. The Russian troll agency also created thousands of tweeting accounts that were masked behind real people and NGOs from the United States. One example is the registered TEN_GOP account, similar to the Republican branch of Tennessee (its true account is TNGOP) which amassed more than 100 000 subscribers. That same year, the intervention in the presidential campaign had begun with publication of materials in support of Trump and Clinton. The slogans ranged from "Ohio wants a prison for Clinton" to "Hilary is Satan, her crimes and lies prove how evil she is."

In the second half of 2016, the Russians were working to prevent minorities from voting. For this purpose, they used slogans such as "The noise and hatred for Trump mislead people and force blacks to vote for Hillary. We cannot choose the lesser of the two evils. It is better for us not to vote at all." Or "American Muslims boycott the current election, most of the US Muslims refuse to vote for Hillary Clinton because she wants to continue the war with Muslims in the Middle East and voted for the invasion of Iraq."[33]

Another working method was to organize demonstrations in the United States. This kind of activity started in 2016. In order to hide their background, Russian trolls presented themselves as activists who could not attend the event personally. In order to attract people, they used their own developed pages and

ads. So, through the account "March_for_Trump," they connected with a real volunteer of Trump's campaign in New York City, who agreed to give them posters for their demonstration. A street demonstration to support Clinton was also held on July 9, 2016.

Despite the fact that Russian cyber operation did not impact the elections results, the outcomes are quite bothering:

- In total, more than 290,000 accounts followed at least one of these pages, the latest of which was created in May 2018.
- The most followed Facebook Pages were "Aztlan Warriors," "Black Elevation," "Mindful Being," and "Resisters." The remaining Pages had between zero and 10 followers, and the Instagram accounts had zero followers.
- There were more than 9,500 organic posts created by these accounts on Facebook, and one piece of content on Instagram.

Table 1. Western and Russian views on cyber war: a comparative view.

Issue	Western concept	Russian concept
Origin	Developed by scholars related to the US military	Developed by Russian security agencies
Conceptual basis	Peace time and War time are separated	There is no distinction between peace time and war time
Scope	Confined to military field	Broader scope, going beyond military
Nature	Primarily technocratic concept with strong emphasis of military issues: strategy, tactics, operations, organization, technologies, doctrines	Primarily oriented to influences on the broader society of the enemy
Time to be waged	In periods of hostilities	All the time, due to the perception of constant conflict and hostile security environment
Tools	Primarily cyber arms	Primarily non-violent, non-armed
Relations with other fields	Autonomous field	Part of the wider field of information warfare
How is organized?	Regular military	Regular army, troll fabrics, media owned by oligarchs close to the Russian president
Cyber actors	Military personnel	Military personell, civilian staff, hacktivists

- They ran about 150 ads for approximately $11,000 on Facebook and Instagram, paid for in US and Canadian dollars. The first ad was created in April 2017, and the last was created in June 2018.
- The Pages created about 30 events since May 2017. About half had fewer than 100 accounts interested in attending. The largest had approximately 4,700 accounts interested in attending, and 1,400 users said that they would attend.[34]

Other Russian cyber operators are media owned by people of the circle of the president Putin. Such a state-oligarchy united front provides the state with additional resources, needed for cyber war as a component of the broader information war. The examined case confirms the conclusion that in Russian strategic thinking, cyberwar and information war are inseparable.

Comparing the Russian and the Western views on Cyber war

The comparison between Western and Russian concepts on hybrid war shows that they are totally different. Table 1 lists the main differences on the basis of the following criteria: origin, conceptual basis, scope, nature, time to be waged, tools, relations with other fields, ways of organization, participants.

Despite the use of the same term, Russian and Western concept deeply differ. It seems that Western experts started realizing this only after the Russian-Ukrainian crisis and the illegal annexation of Crimea. Due to the significant superiority of Russian strategic thinking attained in the last three decades, the West has still to meet this challenge successfully.

References

1 Alexander Kott, Cliff Wang, and Robert F. Erbacher, eds., *Cyber Defense and Situational Awareness*, in *Advances in Information Security*, vol. 62 (Springer, 2015), 111.

2 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Rand Corporation, 2009).

3 "Cyberspace", The United Nations Terminology Database, https://unterm.un.org/UNTERM/dgaacs/unterm.nsf/webview/99b98bdbcbab096185256e620052efd3?opendocument (accessed August 17 2019).

4 Sushil Jajodia, Paulo Shakarian, V. S. Subrahmanian, Vipin Swarup, and Cliff Wang, eds., *Cyber Warfare: Building the Scientific Foundation*, in *Advances in Information Security*, vol. 56 (Springer, 2015), 3.

5 John Arquilla and David Ronfeldt, "Cyberwar is coming!," *Comparative Strategy* 12, no. 2 (1993): 141-165.

6 Julie Mehan, *CyberWar, CyberTerror, CyberCrime and CyberActivism: An In-depth Guide to the Role of Standards in the Cybersecurity Environment*, Second edition (IT Governance Publishing, 2014), 28.

7 The National Institute of Standards and Technology, "Cyberspace," https://csrc.nist.gov/glossary/term/cyberspace (accessed September 9, 2019).

[8] John Arquilla, and David Ronfeldt, "Cyberwar is coming!" *Comparative Strategy* 12, no. 2 (1993): 141-165.

[9] Libicki, *Cyberdeterrence and Cyberwar*.

[10] Libicki, *Cyberdeterrence and Cyberwar*, xv.

[11] Libicki, *Cyberdeterrence and Cyberwar*, xvi.

[12] Libicki, *Cyberdeterrence and Cyberwar*, 117.

[13] Libicki, *Cyberdeterrence and Cyberwar*, 97.

[14] Mehan, *Cyberwar, Cyberterror, cybercrime,* 29-30.

[15] Daniel Ventre, ed., *Cyberwar and Information Warfare* (John Wiley & Sons, 2012).

[16] John McCain, "Cyberwar – the only sphere, in which Russia is ahead of US," interview by CNN, reported by RT, December 12, 2016, in Russian, https://russian.rt.com/inotv/2016-12-19/Makkejn-Kibervojna--edinstvennaya-sfera (accessed September 9, 2019).

[17] Nicu Popescu and Stanislav Secrieru, eds., "Hacks, Leaks and Disruptions: Russian Cyber Strategies," *Chaillot Paper* 148 (Paris: European Union, Institute for Security Studies, October 2018), https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

[18] "Doctrine of National Security of the Russian Federation, approved by the President of RF on 9 September 2000," in Russian, http://base.garant.ru/182535/#friends (accessed on September 9, 2019).

[19] "Doctrine of National Security of the Russian Federation," Presidential order № 646, in Russian, December 5, 2016, https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (accessed on September 9, 2019).

[20] Stephen Blank, "Cyber war and information war a la russe," In *Understanding Cyber Conflict: Fourteen Analogies,* eds. George Perkovich, and Ariel E. Levite, Georgetown, University Press, 2017), 1-18, https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch5.pdf.

[21] James R. Clapper, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee," *Senate Armed Services Committee* (2016): 6-7, http://fas.org/irp/congress/2015_hr/022615clapper.pdf.

[22] "In the Ministry of Defence, RF Created Troops for Informational Operations," in Russian, *Interfax*, February 22, 2017, https://www.interfax.ru/russia/551054.

[23] "Russia is Surprised to Be in Cyberwar against Netherlands," in Russian, *Pravda.Ru*, November 4, 2018, https://www.pravda.ru/news/districts/1396159-russia/.

[24] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare (1Rev)," No. DOP-2016-U-014231-1Rev (Center for Naval Analyses Arlington United States, 2017), https://apps.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf.

[25] "Military Doctrine of the Russian Federation," approved by RF Presidential edict on February 5, 2010, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf (accessed on September 9, 2019).

[26] Connell and Vogler, "Russia's Approach to Cyber Warfare (1Rev)," 1-32, CNA.

[27] Connell and Vogler, "Russia's Approach to Cyber Warfare (1Rev)."

[28] Alexandra Garmazhapova, "Where Do Trolls Live. And Who Feeds Them," in Russian. *Novaya Gazeta*, September 7, 2013, https://www.novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit.

[29] "A Mole Among Trolls: Inside the Internet Research Agency," *VoA news*, April 20, 2018, https://learningenglish.voanews.com/a/a-mole-among-trolls-inside-the-internet-research-agency/4356320.html.

[30] "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election," October 7, 2016, Official website of the Department of Homeland Security, https://www.dhs.gov/news/2016/10/07/joint-statementdepartment-department-homeland-security-and-office-director-national.

[31] Evgenia Kotlyar, "We Had a Goal… to Cause Unrest: Interview with the Ex-collaborator in a Troll Factory in St. Petersburg," in Russian, *TV Rain*, October 14, 2017, https://tvrain.ru/teleshow/bremja_novostej/fabrika-447628/.

[32] Jeff Seldin, "Russia's 2016 Election Meddling More Comprehensive than Realized," *Global Security*, December 17, 2018, https://www.globalsecurity.org/intell/library/news/2018/intell-181217-voa01.htm.

[33] "United Muslims of America" social media accounts, November 2016.

[34] "British Report: Fake News on Social Networks Displace the Real Ones," in Russian, *BBC*, July 30, 2018, https://www.bbc.com/ukrainian/news-russian-45000094.

About the Author

Yavor **Raychev** holds a bachelor degree in Italian Philology from the University of Sofia "St. Kliment Ohridski" and a master in European and International Relations from the University of Linköping, Sweden. Currently, he is finishing his PhD in International Relations at the University of Granada, Spain. His interests include hybrid war, cyber war, international relations, diplomacy and Russia-NATO relations. He provides political analyses for several Bulgarian websites and media.