Journal of International Eastern European Studies/Uluslararası Doğu Avrupa Araştırmaları Dergisi, Vol./Yıl. 1, No/Sayı. 1, Summer/Yaz 2019) ISSN: 2687-3346

Russia's Information Warfare and the Security of Europe

Muhammet Koçak*

(Article Sent on: 21.11.2018/ Article Accepted on: 01.07.2019)

Abstract

Russia's interference to Ukraine in 2014 and the ensuing tensions between the Europe and Russia afterwards have demonstrated the gravity of the geopolitical competition in the region. In this article, I examine the interaction between the Europe and Russia from the perspective of information warfare. Two of the most important components of Russia's information warfare are cyber-attacks and propaganda measures. I analyze these two components of Russian foreign policy strategy, demonstrate their impact in Russia's foreign policy actions and evaluate Europe's ability to counter the threat.

Keywords: Russia, Warfare, Europe, Ukraine.

Introduction

Russia's revisionist foreign policy actions significantly threaten the security of Europe. During the last two decades, Russia employed a combined effort of disinformation and cyberwarfare in Eastern Europe and post-Soviet space on multiple occasions. This paper problematizes Russia's usage of such non-material means that are used in order to advance its foreign policy agenda in Europe.

Russia has inherited a way of approaching to information and battling at information sphere through propaganda and technology from the Soviet Union. Propaganda played a significant role in the survival of Soviet state. Domestically, propaganda is used to "educate" public. In foreign policy, the

* PhD Candidate, Florida International University, mkocak@yandex.ru.

Soviet state aimed to disseminate communist propaganda and subvert Western societies.

After the demise of the USSR, Russia adapted Soviet information warfare to the conditions of the post-Cold War international relations. After the Cold War, the Russian sphere of influence reduced in the Eastern Europe but Russia's capacity to be effective in information warfare increased. Within the framework of the efforts to reclaim its sphere of influence, Russia has developed a full-fledged strategy in order to combine its approach towards information security with its military strategy.

Russia has demonstrated its skills on various occasions during the last decade across the Eastern Europe. Cyberattacks to Estonia, Georgian War and Russia's interference to Ukraine were instances where Russia effectively employed battle in information sphere. One of the most interesting features of these instances was that Russia could deny involvement in information warfare.

Russia's Approach to Information Warfare

Historical Background

Propaganda has been a central instrument of foreign and domestic policy making starting from the early years of the Soviet Union. Earlier indications of the importance of propaganda can be found within the original writings of Lenin. In his essay *No Compromises*? Lenin argues that the Soviet Union was trying to defeat the international bourgeoisie, which is 'stronger enemy,' and to do that, unusual methods such as utilization of conflict of interests or compromise to unstable allies can be used.[1] The Soviet administration aimed to control the flow of information inside the country through censorship and public diplomacy. The institution that was responsible for this task was *Agitprop* (agitation and propaganda). The agitation part was towards the

[1] Vladimir Lenin, *'Left Wing' Communism: An Infantile Disorder* (Moscow: Progress Publishers, 1981), 62.

emotions of the receiver, while the propaganda was for the mind. Using theater, silent cinema and colorful picture posters; *Agitprop* successfully reached to largely illiterate Soviet citizens.[2] Under Stalin, the censorship mechanism went as far into the period of Great Terror, which involved the purge in the Communist Party.

While initially the propaganda machinery was directed towards the population of Soviet Union, it gradually developed to extend Soviet influence abroad, becoming one of the cornerstone dimensions of its foreign policy. Soviet Union funded initiatives that would criticize Western democracies and advertise Soviet Union. Within the framework of this policy, Soviet Union supported the peace movements in Europe that target the US nuclear program and utilized famous Western thinkers and artists. For example, Bernard Shaw, who visited the Soviet Union in the 1930s at the height of Stalin's massacres advertised that the Soviet Union was misrepresented in the West.[3]

Russia's Adaptation of Soviet-era Propaganda to Information Warfare

Within the framework of Cold War's bipolar international system, the USSR could provide security umbrella as well as economic assistance to several nations around the world and lead a pole in the bipolar structure with the help of its nuclear arsenal. Today's Russia, however, faces a different international political environment. It must deal with a relatively stronger opponent in an international system moving towards multipolarity. Therefore, Russia now considers the post-Soviet region as its sphere of

[2] Vladimir Brovkin, *Russia After Lenin: Politics Culture and Society, 1921-1929* (London: Routledge, 1998), 81.

[3] Victoria Drey, "Bernard Shaw: I can't die without having seen the USSR," *Russia Beyond the Headlines*, July 26, 2016, Accessed on August 1, 2019. https://www.rbth.com/arts/literature/2016/07/26/bernard-shaw-i-cant-die-without-having-seen-the-ussr_615147.

influence and the destabilization of the US hegemony on the rest of the world benefits Russia.

Russia's understanding of information space is inherited from the Soviet Union, which considered the information as a domain to be conquered. In contrast to the US, which sees cyberspace as a separate domain, for Russia it is the extension of real battleground. Thus, war at cyber sphere is about dominating information sphere for Russia.[4] Although cyber is an essential part of this war, it is considered within the framework of information warfare.

The Color Revolutions could be considered as a turning point for Russia's increasing its propaganda efforts and putting special emphasis on information warfare. From the point Kremlin observed the impact of NGO's in harming friendly regimes, Russia has increased its efforts in information sphere. Russia has considered soft-power and its organs as a western-centric attempt to meddle in the domestic affairs of Russia and reduce Russia's influence in the Eastern Europe.[5] Putin stated that the activities of pseudo-NGO's are often employed under the name of soft power to create instabilities within the sovereign states.[6]

Today's Russia have a number of advantages in waging an information warfare compared to its predecessor Soviet Union. Russia's natural resources come in handy when financing a foreign policy adventure or resisting to sanctions. Today's communication technology provides opportunities for extensive surveillance and data collection. The post-Cold War liberal environment facilitates the infiltration of Russian propaganda to

[4] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: Center for Naval Analyses), 5.

[5] Jeanne L. Wilson, ''Russia and China Respond to Soft Power: Interpretation and Readaptation of a Western Construct,'' *Politics* 35, no. 3-4 (2015): 291.

[6] Vladimir Putin, "Rossiya i Menyayushchiysya Mir," *Moskovskie Novosti*, February 27,2011.

the world and makes societies and governments more vulnerable.[7] Finally, Russia inherited a free and relatively quality education system from the Soviet Union. Yet, the corrupt economy and inefficient bureaucracy resulted in many people with decent computer and math skills looking for jobs. These people are suspected to be employed by Russia's relevant security organizations to be utilized in cyber operations.[8]

As explained by Herpen, there are three components of the process of how Russia employs propaganda: *Mimesis, Rollback* and *Invention*. *Mimesis* refers to the way Russia faces the threats of western soft power organs. Institute for Cooperation and Democracy, that copies the Goethe Institut could be considered an example to that. *Rollback* refers to the ban of western soft power organs. The arbitrary measures on civil society organization could be considered in that perspective. Lastly, *Invention* refers to putting forward of Russian made soft power machinery.[9] Hiring Western PR firms and feeding thousands of Internet trolls on social media could be considered examples for *Inventions*.[10]

Russia adopts a holistic approach, officially uses the term *informationization,* hence considering information as a domain.[11] In an essay published in a military journal, Russia's Chief of Staff Valeriy Gerasimov suggests that the regime collapses in Middle East and North Africa happened as a result of information

[7] Marcel H. Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (New York: Rowman And Littlefield, 2015), 3.
[8] David Smith, "How Russia Harnesses Cyber Warfare." Defense Dossier American Foreign Policy Council, Issue 4 (August 2017).
[9] Herpen, 33.
[10] Simon Shuster And Sandra Ifraimova, "A Former Russian Troll Explains How to Spread Fake News" *TIME,* March 14, 2018, Accessed on August 2, 2019.
[11] Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia" *US Department of Defense,* June 16, 2017, Accessed on March, 25 2019. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850.

warfare.[12] On December 5, 2016, Russian Defense Ministry promulgated the latest ''Doctrine of Information Security of the Russian Federation.'' It also defines information sphere as a platform, which involves information, the Internet, entities generating information and set of mechanisms regulating public relations in this sphere. The document suggests that it is in the national interest of Russian state to protect its information infrastructure, develop the sector of information technologies and revitalize its national interests in the information security. It also points out that certain states as well as non-state actors use information sphere for military purposes by destabilizing internal political and social situation in various regions across the world. The most important part of the doctrine is the legitimization of Russian security forces to countering these threats by improving Russia's technological capability and countering information threats.[13] Therefore, it can be suggested that Russia sees information as a platform, which can be operationalized to disorganize enemy's governance, shape public opinion in an adversary country and organize protests against the incumbent government.[14]

During the past decade, there has been multiple instances where cyber operations (or information warfare) played a significant role in Russia's entanglements with other states. The investigations could not tie the involvement of Russian hackers or Kremlin-led operative forces to the operations as a result of cyber

[12] Valery Gerasimov, "Tsennost' Nauki v Predvidenii." *Voenno Promıshlenniy Kur'er* no. 476, 8 (2013).

[13] Vladimir Putin, "Ukaz Prezidenta Rossiyskoy Federatsii Ob Utverzhdenii Doktriny Informatsionnoy Bezopasnosti Rossiyskoy Federatsii," *Prezident Rossii,* December 5, 2016, Accessed on August 1, 2019. http://kremlin.ru/acts/bank/41460.

[14] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows,* Accessed on August 1, 2019. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

proxies.[15] In the next section, I examine multiple instances where Russia was suspected to employ information warfare.

Russia's Interference to Europe

Estonia

One of the first manifestations of Russia's information warfare was the DDoS attacks on websites of Estonian government and banks in 2007. As a result of this, a number of Estonian websites could not be reached for a period of time. When the attack happened, the Estonian government was in the process of relocating a Soviet WWII memorial.[16] The second wave of attacks has happened on May 8, 2007 when the victory of Soviet armies over the Nazis was commemorated. During the cyberattacks, Russian Federation Council called for economic sanctions against Estonia and the Estonian Embassy in Moscow was raided.[17] Kremlin denied responsibility but the timing of the attack and concurrent events that happened during the cyberattacks point to Russia.

Georgia

Similar course of events has taken place during Russia's Five-Days War with Georgia in 2008. Georgia's intervention to South Ossetia brought about Russian military intervention to Georgia. During the short war, Georgia was targeted by cyberattacks. The attacks were coordinated with Russian army's advances. As Russian army advanced inside Georgian territory, the website of the then Georgian President Saakashvili was rendered inoperable

[15] Connell and Vogler, 12.
[16] "Behind the Estonia Cyberattacks," *Radio Free Liberty,* March 6, 2009, Accessed on November 25, 2017. https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html.
[17] Connell and Vogler, 15.

for a day.[18] Just before the air attacks to the city of Gori, the websites of the government and media of the city were targeted.[19] As usual, Kremlin denied responsibility, even though the sources of the computers were traced to Russia.[20]

Ukraine

From the initiation of the crisis between Russia and the Ukraine following the departure of Russian-backed Ukrainian President Yanukovich, Ukraine has been targeted by cyberattacks of various nature. Russia has annexed Crimea and demonstrated military presence in Eastern Ukraine. Amid the conflict, the Ukrainian telecommunication infrastructure was intercepted preventing effective communication within the Ukrainian military.[21] During anti-government protests in Ukraine, a malware named 'Snake' harmed the computer network in Ukrainian government.[22] As the conflict between two countries went on, the attacks continued too. As late as Spring 2016, the Ukraine's power grid was targeted by hackers, which caused blackouts.[23]

[18] Jeffrey Markoff, "Before the Gunfire, Cyberattacks," *NY Times*, August 12, 2008. https://www.nytimes.com/2008/08/13/technology/13cyber.html, (Date of accession: November 26, 2018).

[19] Daniel Connelly, "Georgian Cyber Attack (2008)," in Paul Springer. (Ed.), *Encyclopedia of Cyber Warfare*. (Santa Barbara: ABC-Clio, 2017).

[20] Connell and Vogler, 17.

[21] Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs* 1, 1 (2015).

[22] David Sanger and Steven Erlanger, "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government." *New York Times* March 8, 2014, Accessed on August 1, 2019. https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html.

[23] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired,* March 3, 2016, Accessed on December 20, 2018. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Conclusion

The developments in communication technology have revolutionized international politics, security and strategy. Today, the foundations of our security are undermined because of our reliance of cyber networks. The convenience of the delivery of information through cyberspace worries governments.

Russia is one of the countries that are committed to protecting their cyberspace as well as using cyberspace for military purposes. Approaching cyberspace from a perspective of information security, Russia finds free flow of information very dangerous for the sovereignty of the Russian state as well as its influence in Eastern Europe. Besides controlling its information space, Russia is also utilizing cyberspace in order to forward the Russian state interests.

The power vacuum that emerged after the collapse of the Soviet Union have motivated the EU to include the whole Eastern Europe under the EU umbrella. While the political logic of such move is a matter of another discussion, the harm of enlargement to the coherence of the EU has proved to be very immense. Today, the EU member countries include both Bulgaria and Germany, two countries that are economically and politically very different. This creates a structural heterogeneity, which makes it hard for EU to respond to the current threats.

Bibliography

"Behind the Estonia Cyberattacks," *Radio Free Liberty,* March 6, 2009, Accessed on November 25, 2017. https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html.

Brovkin, Vladimir, *Russia After Lenin: Politics Culture and Society, 1921-1929* (London: Routledge, 1998).

Connell, Michael and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: Center for Naval Analyses).

Connelly, Daniel, "Georgian Cyber Attack (2008)," in Paul Springer. (Ed.), *Encyclopedia of Cyber Warfare*. (Santa Barbara: ABC-Clio, 2017).

Drey, Victoria, "Bernard Shaw: I can't die without having seen the USSR," *Russia Beyond the Headlines*, July 26, 2016, Accessed on August 1, 2019. https://www.rbth.com/arts/literature/2016/07/26/bernard-shaw-i-cant-die-without-having-seen-the-ussr_615147.

Galeotti, Mark, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows,* Accessed on August 1, 2019. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Gerasimov, Valery, "Tsennost' Nauki v Predvidenii." *Voenno Promıshlenniy Kur'er* no. 476, 8 (2013).

Lenin, Vladimir, *'Left Wing' Communism: An Infantile Disorder* (Moscow: Progress Publishers, 1981).

Markoff, Jeffrey, "Before the Gunfire, Cyberattacks," *NY Times*, August 12, 2008. https://www.nytimes.com/2008/08/13/technology/13cyber.html, (Date of accession: November 26, 2018).

Putin, Vladimir, "Rossiya i Menyayushchiysya Mir," *Moskovskie Novosti,* February 27,2011.

Putin, Vladimir, "Ukaz Prezidenta Rossiyskoy Federatsii Ob Utverzhdenii Doktriny Informatsionnoy Bezopasnosti Rossiyskoy Federatsii," *Prezident Rossii,* December 5, 2016, Accessed on August 1, 2019. http://kremlin.ru/acts/bank/41460.

Sanger, David, and Steven Erlanger, "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government." *New York Times* March 8, 2014, Accessed on August 1, 2019. https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html.

Shuster, Simon and Sandra Ifraımova, "A Former Russian Troll Explains How to Spread Fake News" *TIME,* March 14, 2018, Accessed on August 2, 2019.

Smith, David, "How Russia Harnesses Cyber Warfare." Defense Dossier American Foreign Policy Council, Issue 4 (August 2017).

Thomas, Timothy L., "Nation-State Cyber Strategies: Examples from China and Russia" *US Department of Defense,* June 16, 2017, Accessed on March, 25 2019. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850.

Unwala, Azhar, and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs* no.1, 1 (2015).

Van Herpen, Marcel H., *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (New York: Rowman And Littlefield, 2015) 33.

Wilson, Jeanne L., ''Russia and China Respond to Soft Power: Interpretation and Readaptation of a Western Construct,'' *Politics* no. 35, 3-4 (2015).

Zetter, Kim, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired,* March 3, 2016, Accessed on December 20, 2018. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.