DOI: 10.53477/2668-2001-21-16

LANDMARKS OF RUSSIA'S USE OF INFORMATION WARFARE

Alina Prelipcean[1]
"Carol I" National Defence University
Andrei Albert
"Carol I" National Defence University

Abstract

Russian Information warfare represents an extended concept that covers a wider and more diverse range of actions when compared to NATO's approach on information operations. Russian techniques, tactics and procedures in the field of information warfare do not differ much from those used in the Soviet period but are adapted to the new technological achievements. The specific means of use the information warfare are acquired by the future politico-military leaders of the Russian state starting with their preparation period at an age of accumulation. On short and medium term, it is likely that Moscow's activities specific to the information warfare will increase being favored by the limitations imposed by the Covid 19 pandemic.

Keywords: information operations; information warfare; special propaganda.

INTRODUCTION

Sun Tzu stated that "all warfare is based on deception. That is why (...) lure the enemy to trap him; feign disorder and crush him; avoid him where he is strong. Pretend inferiority and encourage his arrogance. Don't weaken him for a moment, harass him" (Sun Tzu 1976, 24-33)

Vladimir Putin stressed that "Russia's approach to future conflicts, which will be asymmetric, is one based on intellectual superiority" (Presamil.ro 2017)

The transformations that took place at the beginning of the 21st century, generated mainly by technological evolution, have influenced the way wars are conducted. Thus, conflicts no longer take place only in trenches, through conventional military actions, but have as a *"battlefield"* the online environment, being won essentially by having information supremacy (Intelligence.sri.ro 2019).

This thesis was developed on the basis of consultation of open sources that address the issue of Russia's information warfare as well as through analytical research carried out by authors that led to the formulation of conclusions and assessments presented in this paper.

Information warfare involves the use of diversion, manipulation, disinformation and distortion of reality, the numerical force being replaced by troll armies. Thus, achieving the proposed objectives or promoting one's own interests can be achieved by altering the reality which in turn is achieved by changing people's opinions (Intelligence.sri.ro 2019).

Even though the information warfare has a long tradition in Russia, recent years have marked a shift using geopolitics as the main foundation. Political geography offered Moscow ideological arguments in its strategy to confront "the West." Unlike the ideology of liberalism, Moscow promotes a neoconservative post-liberal power that fights for a just multipolar world, defending tradition, conservative values and true freedom. These elements were the basis for justifying Ukraine intervention, namely the annexation of Crimea, in the context of rivalry between "Eurasian civilization" and "US-led Atlantic civilization" (Darczewska 2014).

[1] Corresponding author: alina_prelipcean@yahoo.com

RUSSIAN PERSPECTIVE ON INFORMATION WARFARE

According to RAND corporation, "information operations known as influence operations includes (…) the dissemination of propaganda in pursuit of a competitive advantage over an opponent" (Schville, Atler, Welch, Baffa, and Paul 2020).

The Russian Federation's perspective on information warfare (*informatsionaya voyna*) is rooted in Soviet thinking which defined the concept by the phrase "special propaganda" (*''spetspropaganda''*) (Porotsky 2019, 6-19).

Currently "information warfare is a holistic concept that includes psychological operations (PSYOPS), electronic warfare, computer network operations and information operations" (Porotsky 2019, 6-19). Some of the elements that frame the current concept of information warfare are also found in the methods used by the Soviet Union in the action plans generically called "active measures". Russian Federation military doctrine, developed in 2010, stated that information operations aim to "achieve political objectives without the use of force". (Porotsky 2019, 6-19)

In contrast to NATO's approach, the Kremlin's angle is different in terms of complexity. Thus, we note that for the Russian Federation, all areas form a unit under the concept of "information warfare" while NATO approaches the concept of "information operations". (Scîrlet and Ichimescu 3/2020).

Moscow considers information, implicitly information warfare, as a "dangerous weapon" due to its characteristics: low costs, easily accessible, penetration into target environments without taking into account borders (Darczewska 2014).

Russia's perspective on information warfare refers to influencing the consciousness of the masses as part of the existing rivalry between various international actors in the information space, by use of special means to control information resources as "information weapons". Moscow mixes by definition the information and cyber space, appealing to psychological warfare between East and West and to geopolitical elements specific to the Cold War. (Darczewska 2014)

In Russia there are two geopolitical schools of thought whose representatives, Igor Panarin and Aleksandr Dughin, approached information operations as part of the information warfare. The perspective promoted in both schools of thought reveals that information warfare is a means by which states achieve their goals internationally or regionally or in terms of domestic policy, thus gaining geopolitical advantages.

The work of I. Panarin and A. Dughin focuses on two levels, as follows:

- raising public awareness in Russia of the "external threats" that exist in the information environment;
- setting up a system to respond to these threats from an information point of view. (Darczewska 2014).

I. Panarin and A. Dughin are "both theorists and practitioners of information warfare" through analytical programs and programs produced on Russian TV stations: *''NTV'', ''Channel 1'', ''Ren-TV'', ''TVRT''*. At the same time, radio stations from the Russian Federation, such as the *''Voice of Russia''*, host shows produced by I. Panarin with suggestive titles (*''Global Policies''* and *''Window to Russia''*) where aspects of domestic and international politics are approached and commented. (Darczewska 2014)

PARTICULARITIES OF THE RUSSIAN INFORMATION WARFARE

Russia's information strategy aims internally to mobilize society and externally to rebuild the sphere of influence in the former Soviet space. From Moscow's perspective, two key factors are essential to information operations success: the existence of the Russian diaspora, receptive to Kremlin propaganda, and the use of Russian language in the information environment. (Darczewska 2014)

In Russia, information operations are treated as an interdisciplinary science since it covers a very broad range of actions targeting political, social, military, diplomatic, psychological, intelligence and counterintelligence domains. (Darczewska 2014).

A number of educational institutions and research centers deal with the issue of information operations such as the Information Security Institute at Lomonosov Moscow State University. Students of this institute are trained in the history and economics of the former Soviet states, the social movements and political representation of the Russian diaspora and ways of cooperation with their representatives. It should be noted that among the lecturers of this institute are people like Maxim Meyer, media strategy specialist and executive director of the Rusky Mir Foundation, who actively supports Russian communities abroad. (Darczewska 2014)

Another example at the institutional level is the Military Information and Foreign Language Department of the Military University of the Ministry of Defense of the Russian Federation. The changes within this institution are suggestive of an understanding the way Moscow relates to special propaganda. Thus, the subject entitled *Spetspropaganda* was removed from the curriculum in the 1990's to be reintroduced in 2000 when the institution was reorganized.

Currently, specialists are training in "organizing foreign intelligence and military communication" and "monitoring and developing military intelligence." Special propaganda is learned within the institution by both military and civilian personnel, such as journalists and war correspondents (Darczewska 2014).

Also, the Moscow State Institute of International Relations (MGIMO) and the Diplomatic Academy of the Ministry of Foreign Affairs, where future Russian diplomats are trained, have in their curriculum in addition to sociology, philosophy and political science subjects such as: network communication technology, information and network war and situation analysis. The subject of information warfare has been given the status of an academic science. (Darczewska 2014)

The early writings given by the professor Igor Panarin at the Diplomatic Academy formed the basis of the Information Security Doctrine of the Russian Federation. In this context, I. Panarin described two major forms of aggression against Russia, as follows:

- the first form began with the launch of the Perestroika reform program and ended with the collapse of the Soviet Union.

- the second form started at the beginning of this millennium and will last until 2020 when Eurasianist ideas will prevail. (Darczewska 2014)

In his book, "*The Second Information War - War on Russia"*, I. Panarin argues that "all the colorful revolutions in the former Soviet Union and the Middle East are a product of the information aggression and social control technologies used by the United States" (Darczewska 2014)

In the same volume, I. Panarin defines the terms used in information operations of the Russian Federation, as follows:

- manipulation of information: the use of authentic information in a way that produces false implications;
- social control: influencing society;
- disinformation: dissemination of fabricated or manipulated information;
- fabricated information: creating and promoting false information;
- information manipulation: using authentic information in a way that gives rise to false implications;
- social maneuvering: intentional control over the target audience in order to obtain certain advantages. (Darczewska 2014)

According to I. Panarin, the tools used in information operations can be divided into secret and open. These include: "propaganda (black, gray and white), information (structures that gather information about the opponent), analytical component (media monitoring, current situation analysis) and organizational component (coordination of media channels, media influencers to influence politicians' opinions and the media in general to achieve the results desired by the state involved in the information war)". In addition to these tools, I. Panarin also mentions "other combined channels" including the use of special operations forces for sabotage missions conducted under a foreign flag. (Darczewska 2014)

I. Panarin distinguishes the following stages in the process of information operations management: forecasting and planning, organization and stimulation, feedback, operation adjustment and performance control. (Darczewska 2014)

Russian techniques, tactics and procedures in the field of information warfare do not differ much from those used in the Soviet period with the mention that they have been adapted to the new tools that technology has made available. Thus, in order to achieve its goals, Moscow uses both state-controlled media, such as ‘’*Russia Today”* or ‘*’Sputnik”*, as well as a community of hackers or trolls coordinated by the Russian intelligence structures (Jonas and Chabuk 2018).

Another channel of interest from an information operation perspective, in a globalized and interconnected world, is the Internet and especially social networks, despite the fact that some of them are outside of Kremlin’s control. Thus, Russia used the social network Facebook to promote spots with the Black Life Matters movement while officially categorizing the same entity as a dangerous threat. (Jonas and Chabuk 2018). Black Lives Matter is a decentralized political and social movement protesting against incidents of police brutality and all racially motivated violence against black people.

According to figures circulated during the hearings in the US Parliament (House Intelligence Committee), the Internet Research Agency (IRA) in Saint Petersburg is responsible for the financing of approximately 3,500 spots on Facebook in order to influence an audience of approximately 11 million US users (Jonas and Chabuk 2018). IRA is a Russian troll farm in St. Petersburg, in essence a Kremlin backed enterprise staffed with hundreds of people whose main job is to sow disinformation on the internet (Calamur 2018).

In an attempt to influence the target audience in various states, from US, UK to the Baltic States, Russia has used the online environment to create confusion, to cause ethnic tensions or erode trust in democratic institutions. As an example, the Kremlin financed spots on Facebook also for ‘’*Blue Life Matters’* movement *(*which represents a countermovement started in response to *Black Life Matters)*. In this case, Russia's goal was not to get involved in a US internal dispute in order to impose its own position, but to exploit the existing social division to create an atmosphere of general suspicion in society (Jonas and Chabuk 2018).

CONCLUSIONS

The information warfare of the Russian Federation represent another level of the hybrid approach of conflicts. Along with the use of private military companies, information warfare allow the achievement of Moscow's objectives without a direct involvement of the state. The possibility of a plausible denial of information aggression favors Kremlin's impunity.

The main difference between Soviet propaganda and the information warfare waged currently by the Russian Federation is that Moscow no longer seeks to proclaim an absolute truth but to distract, confuse, polarize and demoralize.

The tactics, techniques and procedures by which Moscow wants to influence public opinion and through this political agenda in various countries are constantly changing, being permanently adapted for a better penetration of the target audience.

In the context of Covid-19 limitations, the relatively low costs of the activities in the information environment compared to those of a conventional aggression represent pre-requisites for the intensification, on a short and medium term, of the information warfare waged by Russia.

REFERENCES

Adam, Taylor. 2016. *Analysis. Is There a Link between Putin’s Approval Rating and Aggressive Russian Foreign Policy*?. Washington Post. https://www.washingtonpost.com/world/2018/11/26/is-there-link-between-putins-approval-rating-aggressive-russian-foreign-policy/

Calamur, Krishnadev. 2018. Feb. *What is the Internet Research Agency.* .https://www.theatlantic.com/intenational/archive/2018/02/russia-troll-farm/553616/

Darczewska, Jolanta. 2014. May. *The Anatomy of Russian Information. The Crimean Operation, a Case Study*. osw.waw.pl/en/publikacje/point

https://presamil.ro/razboiul-informational-dus-de-rusia. 2017. Bucharest: Press Department Romanian Ministry of Defense, Russian Information Warfare

Jonas, Adam, and Chabuk, Timur. 2018. September 1st. *Understanding Russian Information Operations*. www.afcea.org

Scîrlet, Petre, Ichimescu, Cristian. 2020. *Conflictele/Operatiile informationale ale Federației Ruse în contextul Sars-Cov-2.* Bucharest: Magazine Gandirea Militara Românească, nr.3.12.

Porotsky, Sophia. 2019 June 10th. *Analyzing Russian Information Warfare and Influence Operations.* 6-19*.* https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/

Razboiul 2.0. 2019, March 13th. https://intelligence.sri.ro/razboiul-2.0

Schville, Michael, Atler, Anthony, Welch, Jonathan, Baffa, Richard, and Paul, Christopher. *Improving Intelligence Support for Operations in the Information Environment*. www.rand.org/ InformationOperations

Sun Tzu. 1976. *Art of Warfare*. Bucharest, Military Publishing House. 24-33.