DOI: 10.53477/2971-8813-22-61

RUSSIA'S APPROACH TO CYBERSPACE

Claudiu-Cosmin RADU
Lieutenant Commander, Ph.D. Student, "Carol I" National Defence University,
Bucharest, Romania
radu.claudiu@unap.ro

Abstract: *In recent years there have been important changes in the approach to conflict, leading to a paradigm shift in the future warfare. Cyberspace has become a serious challenge for all states. Being easy to connect and cheap to operate, it has become a preferred battlespace for many actors. It is used to disrupt networks, destroy and steal data, block or slow down critical infrastructure or spread false information. The development and innovation of military technologies and the professionalization of soldiers are not enough to fight in information warfare. Revising and improving old doctrines, and strategies is a clear form of supporting new techniques, tactics, and procedures of the Russian fight in cyberspace. The improvement of conventional tactics of warfare in conjunction with the introduction of new unconventional tactics of warfare has predictably led to the strengthening of internal, regional, and global security and resilience. The new vision of Russian warfare is that kinetic actions are supported by non-kinetic ones. As a result, Russia's cyber activity has recently intensified amid the invasion of Ukraine, putting the whole world on alert. Malicious activity in cyberspace is creating large-scale disruption in all areas. In this context, the activation of Article 5 for attacking a Member State in cyberspace is becoming increasingly discussed.*

Keywords: *cyberspace; information space; security; strategy; doctrine; Russian Federation; Ukraine.*

Introduction

In recent decades, the rapid development of modern information and communication technologies has had a major impact on modern society, irreversibly transforming the way the economy, culture, politics, industry, conflict, and the everyday life of the individual operates. Whereas at the end of the 20th-century people could more easily access personal computers at ever-lower prices, the beginning of the 21st century is characterized by increasing connectivity, i.e., the integration of computers into local networks. They have evolved from a purely administrative tool supporting the optimization of bureaucratic processes to a strategic tool widely used in all areas, critical and less critical. Today, easy access through the globalization of communications and access to information from anywhere in the world can be one of the principles for the development and proper functioning of modern society. The information society represents a new stage in the development of human society, in which knowledge and information play a key role.

In the information society, the main resource of power is information, as valuable as material, financial or human resources. Information is also an important factor in determining a state or non-state actor’s power as well as the driving force behind the modern knowledge-based society development.

Intelligence is reflected in a state's military, economic, or financial power, but the ability to obtain, store, and process specific information can provide a distinct advantage over adversaries. In the context of specific missions, mastery of intelligence can be critical in achieving success, decisively influencing the physiognomy of military actions during the decision-making process of planning and organizing actions.

The term *cyberspace* was first used by American-Canadian author William Gibson in 1982 in a story published in *Omni* magazine and later in his book *Neuromancer*. In that science fiction novel, Gibson described cyberspace as "*the product of a computer network full of artificially intelligent entities*". (Bussell 2013)

The U.S. Department of Defense defines cyberspace as "*an overarching domain in the information environment consisting of interdependent networks of information technology infrastructure and user data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*". (Government 2018, GL-4) Cyberspace encompasses the identities and objects that exist in computer networks used by human individuals for various purposes.

Cyberspace is limitless, characterized by dynamism and anonymity, with the potential to generate opportunities for the development of the information society, but at the same time, it can also lead to a number of risks. Highly digitized states, which depend heavily on computers, can become very vulnerable, and ensuring the security of cyberspace must be a main concern. "*Attacks on these computers can be as damaging as traditional military attacks. Cyberwarfare has several goals: exploiting others' information for their own purposes (espionage); misleading adversaries; disrupting enemy computer systems or temporarily disabling their use, and destroying those systems.* " (Robinson 2010, 164)

The expansion of cyberspace led NATO to acknowledge it in 2016, through the Warsaw Summit Official Declaration, as an operational environment, joining the other operational environments: land, sea, air, and space: " ... *we recognize cyberspace as an area of operations in which NATO must defend itself as effectively as in the air, on the ground or at sea.* " (North Atlantic Treaty Organisation 2017)

The cyber domain has undergone major changes in a short-term period of time, providing exceptional opportunities, as well as risks for cyberspace users. The sources of risk are represented by some of the actors that populate it, speculating, in the interest of a state/organization or individually, on vulnerabilities specific to the domain.

Today, companies, state and non-state actors, and international organizations are concerned by countering risks, threats, and vulnerabilities addressing the security of the virtual world.

A powerful cyber-society is a one in which computerized data transfer and processing are omnipresent and in which individuals, groups or individuals, or even states, seek to exploit the increased complexity and connectivity of networks of critical infrastructure systems, with the potential to cause significant material damage and financial loss and thus to endanger the *"military, political, economic, cultural or environmental"* (ecological) *security* of the targeted state. (Barry, Ole and Jaap 1997, 22)

Security is the state in which individuals, groups of people organized along different criteria, nation-states, can develop freely under the condition of respecting a system of adopted and recognized (internal and international) rules.

Cybersecurity has become an important matter within countries, leading them to take a series of initiatives in this direction. Currently, most countries in the world have adopted and implemented national cybersecurity strategies, some of which are in the process of being legislated. Implicit in this is the creation of cybersecurity bodies, action lines, inter-institutional cooperation and dialogue plans, and many others.

The purpose of the article is to understand and analyze cyberspace from the Russian Federation's perspective. It also presents a brief comparison of the legislative framework regulating actions in the cyber environment with similar regulations used by Western countries. In order to achieve this goal, I suggest 3 other objectives:

- analysis of concepts such as cyberspace and information space;
- identifying and analyzing the documents that regulate activities in the information space;
- Russia's important activities and *modus operandi* in the information space, with an accent on actions against Ukraine.

1. National Russian Federation framework documents governing the cyberspace

Cyberspace is becoming a complex battlefield of the future, and advanced countries are becoming more concerned about possible negative consequences locally and internationally, focusing on developing and implementing coherent cyber policies to reduce risks, vulnerabilities, and threats, while at the same time seeking global cooperation.

The Russian Federation has always used intelligence and disinformation in its military actions. As a continuation of the Soviet Union, it has used propaganda within the territories to strengthen the population's perception of the leaders and the state. It has also used information operations outside its territories to spread panic among its opponents and to create favorable conditions for combat. (Timur Chabuk 2018)

As cyber threats know no state or organizational boundaries, Russia adopts its own strategies and doctrines to strengthen its national security taking into account its strategic interests.

In the cyber security domain, the dialogue between Russia and international partners is characterized by intransigence and discord, primarily because there is no common vocabulary in rapports of the terms used. Secondly, these disagreements are due to the different rules that Moscow follows, which Russian Communications Minister Igor Shchegolev said: *"for the time being, in the West not everybody always understands what rules we are following"*. (Giles 2012, 64)

However, the most important divergence is the term *"cyber warfare"*, or the Russian equivalent *"information-technological warfare"'*, which is only part of the concept of *"informational confrontation"*. The Russian Ministry of Defense describes informational confrontation as *"the clash of national interests and ideas, where superiority is sought by targeting the adversary's information infrastructure while protecting its own objects from similar influence"*. (Kukkola 2020)

Moreover, this claim is also supported by Kier Giles, one of Chatham House's most distinguished consultants, he argues *"that any research on Russian capabilities and intentions which includes the word "cyber" risks providing fundamentally misleading results"*; instead of *"cyber"*, the Russians use the term *"informational"*. (Kukkola 2020, 101)

Russians consider information to be *artificial* form (i.e. cybernetic) seen as the technical representation of information and *natural information*, which includes thoughts and information from books and documents. In terms of security, the closest Russian word in meaning to the English language is "*protection*". The Russian perspective on information security (INFOSEC) includes several dimensions: human, social, spiritual, and technical (cyber). In addition, an essential aspect of *"information security"* is considered the protection of the population against terrorism and censorship. (Godwin, et al. 2014, 11)

Russian military researchers use the term *cyber* when referring to threats and hostile actions coming from the West but are reluctant to use the term to describe their own activities. Moreover, some authors argue that this choice of terms has a negative meaning since the Soviet Union and that is why the term *information security* is used. The terms *information space* or *information sphere* are used when talking about the *operational environment,* which is much broader than the term used by Western countries to define *cyberspace* or *cyber domain.*

The 2016 "Russian Doctrine of Information Security" defines the information sphere as: *"a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet [...], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security,* *as well as a set of mechanisms regulating social relations in the sphere"*. (Hakala and Melnychuk 2021, 6)

Information space is a sphere of activity related to the formation, creation, transformation, transmission, use, and storage of information, which has an impact on individual and public consciousness, information infrastructure and information itself. (Defence 2011, 5)

The Russian concept of information-technological warfare is very similar to the Western concept on cyber warfare. However, cyber-attacks represent only one part of information-technological warfare, namely electronic warfare. The theory of ideas and systems in the cyber domain gives the Russian approach to cyber warfare a distinct character, as does the distinction between geopolitical informational confrontation and operational-tactical warfare. However, the intentional use of different terms should not obscure the fact that the reality of cyberspace is the same for all who operate in it. (Kukkola 2020, 258)

Russia's desire to return to its great power status leads to obsessive competitiveness with the US and its allies or partners in all areas: political, economic, military, social, technological, and informational, in order to tip the balance of power in its favor. Cyberspace operations have become an important aspect of this competition.

These Russian cyber operations are primarily concerned with cyber laws so that their actions are not followed by repercussions from the aggressor. They also use technical methods and means to avoid accusations of a violation of international law by the state or organization harmed. This accusation may mean determining the identity or location of the attacker. Moreover, the aim of malicious actors is not only to avoid prosecution but also to maintain their anonymity for as long as possible during the cyber operation. Thus, anonymity implies not only the inability to identify an individual, group, or state actor but also *"the inability to recognize that an attack is taking place and the inability to isolate the target or objective of the attack"*. (Jasper 2020, 8-9)

According to Russian cyber researchers, the informational confrontation is ongoing, with Russia using every tactic, technique, and procedure to gain informational superiority in this competition. The tools most commonly used in the cyber environment include psychological operations, electronic warfare (EW), and kinetic actions. In practice, cyberspace can be used for both physical attacks on infrastructure and cognitive attacks such as disinformation. However, the center of gravity in 'informational confrontation' is in people's minds and perceptions of events, both domestically and internationally. (Hakala and Melnychuk 2021, 4)

Russian President Vladimir Putin's regime applies censorship in the cyber environment and methods of controlling people through the internet, publications, and television. He also wants to set up his own RUNET internet to be controlled and used only within the country. Furthermore, he wants to reduce access to the international internet while introducing and using the local one. Moreover, as a security measure, it will be used only in Russian language.

On the other hand, Western countries, democratic and respecting international law, do not consider that the protection of information should be done by censoring information or using any method of misleading the population. The reasoning behind this is the belief that the most aware and educated population is best able to defend itself against harmful information. Finally, the US believes that a government would be acting improperly if it used psychological operations to influence the opinions and perceptions of its citizens. (Godwin, et al. 2014, 12)

In order to understand how the Russian Federation acts in the information domain, I will analyze the most significant strategies and doctrines governing it.

Like most active countries in the cyber environment, the Russian Federation has developed legislation in this area, including a number of strategies, doctrines, and other documents governing the cyber environment. These are developed in line with geopolitical aspirations at the strategic level, the institutional culture of the political, military, and intelligence leadership, and the eternal competition between Russia and the major world powers.

Until the invasion of Ukraine in early 2022, the perception of Russia's war strategy consisted of non-military, non-kinetic actions being able to operate effectively from cyberspace without the use of military force and a significantly lower cost. But even Russian thinkers have written intensively about general and doctrinal strategies for offensive hybrid warfare, resulting in the fact that the future of warfare will be bound to cyberspace and non-kinetic actions that will be a potentiating factor for classical warfare actions.

Between the 1990s and 2000s, a number of articles by military specialists appeared dealing with non-military measures in conflicts. Despite this, it was not until after 2000 that a working group of military theorists and senior military officials was formed who admitted that the line between war and peace had become blurred and nonviolent actions could be so effective that they could be considered violent, turning them into an instrument of war. (Lilly and Cheravitch 2020, 132)

"The Russian National Security Concept" appears in 2000, a Russian Federation vision of the individual, civil society, and nation-state security against internal and external threats from all aspects of life, political, economic, scientific, technological, social, environmental, and informational. Also in the same year, "The Information Security Doctrine of the Russian Federation" was published before the first official US document on cyberspace. This publication deals with the goals, objectives, principles, and basic directions of Russia's information security policy. Moreover, the doctrine, in the Russian sense of *national policy*, is the fundamental document governing Russia's approach to information security and cyberspace concerns. As this document states, it ensures the rights and freedoms of the citizen to *"freely seek, receive, transmit, produce, and disseminate information by any lawful means"*. (Article I, Part 1) Further, the doctrine stipulates *"the development of methods for increasing the effectiveness of state involvement in the formation of public information policy of broadcasting organizations and other public media"*. (Article I, Part 4) General Colonel Vladislav Serstyuk, then First Deputy Secretary of the Security Council of the Russian Federation, responsible for information security and one of the authors of the document, explained that the doctrine would not be used to restrict independent media, but that all media, government or private organization, should be under state supervision. (Giles 2012, 74) This would reduce freedom of expression and lead to veiled censorship by the authorities. This document is also aimed at counter-propaganda activities in order to avoid the negative effects of spreading false information about Russian government policies as well as the implementation of state mechanisms to prevent the psychological effect of the influence of information in the common consciousness of society. These ways of preventing negative effects were tested during the online organization of the 2011 Russian parliamentary elections. (Giles 2012, 75)

After the waves of cyber-attacks on Estonia in 2007, which were reportedly triggered by actors from the Russian territory, the European Union and the North Atlantic Treaty Organization (NATO) have not officially blamed Russia even though Internet addresses including those of Russian state institutions have been identified. In response to these cyber-attacks NATO has established its Cyber Security Centre in Estonia in Tallinn. In the absence of an official indictment, the complicity of the federation remained uncertain. This led in 2008 to the publication of a document signed by President Putin called "The Strategy of

Information Society Development in Russia". This developed Russia's first cyber and information strategy to be used later in cyberspace conflicts.

Subsequently, the Ministry of Defense publishes in 2011 "Conceptual Views on the Activities of the Armed Forces in the Information Space", a document that refers to the "Information Security Doctrine of the Russian Federation" from 2000. This document deals with political threats in information space and the widespread use of electronic systems in the command and control of troops and weapons, based on a set of principles: legality, cooperation with friendly states and international organizations, and limitation and prevention of military conflicts in information space. (Lilly and Cheravitch 2020, 136)

"The Military Doctrine of the Russian Federation" approved by the Russian Federation presidential edict no. 5 in 2010 replaced the previous "Military Doctrine of the Russian Federation" from 2000. According to it, the aim was to develop and improve forces and resources in the field of information space and to implement information warfare measures in advance in order to achieve political goals without using military force. The doctrine also states that operations in the information environment are also used in peacetime and not only in wartime. (Jasper 2020, 72) It also uses the information environment alongside the political, diplomatic, legislative, economic, military, and surrounding environments to protect the national interests and critical infrastructure of Russia and its partners.

"The Military Doctrine of the Russian Federation" updated in 2014 highlights measures on the use of military force to protect its national interests only after political, diplomatic, legal, economic, informational, and other non-violent tools have been exhausted. It is a known fact that informational confrontation is becoming more powerful and its potential is being developed. Military dangers and threats are moving into the information space and the use of information and communication technology is becoming a destabilizing factor on the sovereignty, political independence, and territorial integrity of the state, critical infrastructures, and people. (Kukkola 2020, 181)

Regarding Russia's foreign policy, "The Foreign Policy Concept of The Russian Federation" appears in 2008 according to which Russia will strengthen its international position and establish some equal and mutually beneficial partnerships with all countries. It will further develop its own effective means of influencing public opinion abroad in the information environment and strengthen its role in the media by taking the necessary measures to repel informational threats to its sovereignty and security. In the 2013 updated version, the term soft power appears (Latukhinamaxim and Makarychev 2013) which will inherently lead to more effective use of information space. In order to achieve Russia's foreign policy goals, this tool has become an important asset as presented in the latest 2016 version. Moreover, Russia is trying to ensure that the world has an objective image of the country, and is developing its own effective ways to influence foreign audiences, promote Russian mass-media and Russian-language in the global information space, providing them with the necessary government support. It is proactive in international intelligence cooperation and takes the necessary measures to counter threats to its information security. New information and communication technologies are used for this purpose. Russia intends to promote a series of legal and ethical rules on the safe use of these technologies. The Federation ensures the right of everyone to have access to impartial information. (Russian Federation 2016)

The most important document governing the information space of the Russian Federation is Russia´s new "Information Security Doctrine" of 2016, which replaces the "Information Security Doctrine" published in 2000. It continues the direction taken in previous strategic documents, in which Russia is perceived as a besieged fortress identifying a number of external threats to Russia's information space and calls for intensified monitoring of Russia's internet segment, RUNET. (Pynnöniemi and Kari 2016) This strategic planning document recognizes the role of the information domain in technological progress and national security but also calls for an increased role for the internet, information security, and the development and production of information domain technology. Also, the increase in cyber-attacks by foreign countries for military purposes will be seen as a major negative factor. A major risk identified in this doctrine is Russia's dependence on foreign information, and communication technologies. One mitigation of these risks would be domestic production of software and hardware, but this could take many years, so Russia has decided to strengthen its own RUNET (Pynnöniemi and Kari 2016) Doctrine suggests that a balance should be struck between the rights of citizens to free access to information and limiting the rights arising from the need for national security in relation to the information. The text also highlights the need for continuous monitoring of information security threats and increased control over the Russian segment of the internet by security authorities as part of the response to internal and external threats in the information sphere. A number of amendments to the laws on counter-terrorism require mobile network operators and internet service providers to retain and store data on users, user activity, and their conversations on Russian territory for one year. They are also required to retain and store the content of all users' conversations on Russian territory for up to six months from July 2018 and allow Russian security agencies to decrypt correspondence. (Pynnöniemi and Kari 2016)

President Vladimir Putin has signed a decree on a new strategy for the development of Russia's information society from 2017 to 2030. This document was published on the country's official website and replaces a previous strategy that had been in effect since 2008. "The Strategy of information society development in Russia until 2030" is the fundamental resource for the preparation of doctrinal, conceptual, and other documents defining the objectives and directions of the activities of public authorities, as well as the principles and mechanisms of their interaction with organizations and citizens in the development of the information society in the Russian Federation. The new strategy prioritizes traditional Russian spiritual and moral values and observance of behavioral norms in the use of information and communication technologies. The document also details the concept of *critical information infrastructure* and the need to protect that infrastructure using state anti-hacking resources. In addition, the strategy calls for the use of encryption in all federal electronic mail and the replacement of imported software and hardware with domestic products in all government institutions. (information 2017) The aim of the strategy is to *"improve the quality of life of citizens, ensure Russia's competitiveness, develop the economic, socio-political, cultural, and spiritual spheres of society, improve the system of public administration based on the use of information and telecommunications technologies"*. (Putin 2018)

In addition to these documents, a variety of rules and regulations governing operations in Russian cyberspace have been passed, including the 2019 "Sovereign Internet of Russia" law, which effectively permits the government to disconnect from the world internet at any time. By 2024, the Kremlin hopes that only 10% of Russian internet traffic would be routed through foreign servers. It also sees control over its internal cyberspace as essential to its security. Any threat to cyberspace could be perceived as a threat to state sovereignty. This will lead to the implementation of the concept of "digital sovereignty" by taking steps to secure Russia's internal cyberspace. Digital sovereignty is used in this context primarily as a political term and can be understood as the ability and right of a government to determine its fate within its own information space. (Hakala and Melnychuk 2021, 12)

Looking at Russia's framework documents governing information space, we can recognize the Russian's state desire to maintain a clean, secure, and resilient information space. We also notice the rapid development of information technology and the imbalance between Russia's desire to develop its own communications and information technologies and the use of foreign technologies. Moreover, there is a desire to awaken the nationalist spirit and for the state to cooperate with organizations and citizens, just as in Western countries. The strategies set out elements that enable citizens to navigate and have free access to information. Compared to other democratic states, where people are truly free and equal in cyberspace, here some laws regulating terrorism or regulating the sovereign Internet intervene and under the pretext of security of information space, citizens are restricted. In Western countries, citizens have the right to respect personal data, and the use of such data without personal consent becomes a crime, while the Kremlin has given the law to record and store data, information, including conversations of citizens on Russian territory. The government is restricting information in the media and on the Internet under the same security pretext. It is astonishing that the government has thought of implementing a national, Russian-language Internet in order to isolate the state from the rest of the world, with the consequence of limiting access to and control of information.

2. Russian Federation activities in cyberspace

After the fall of the Soviet Union, Russia tried to regain its superpower status. In the unregulated Russian internet space after this period, the FSB (Federal Security Service) developed cyber activities with the help of individuals or non-state actors whom it has convinced or coerced to work for some government security agencies and helped to develop offensive cyber operations.

The Russians took advantage of the information environment during the second Chechen war in 1999, launching systematic government-coordinated disinformation tactics that helped mobilize the ethnic Russian community and isolate the insurgents in order to frame the war as an anti-terrorist campaign. (Blank 2017, 83) The effective isolation of the Russian media space demonstrates the importance of media control as a strategy for winning a war.

Amid historical disagreements between the Russian Federation and Estonia, culminating in the Estonian government's decision to relocate the statue of a bronze soldier from the center of the capital to a more peripheral location. This statue of the Russian soldier had important historical and cultural significance for Russians, as it represented the Soviet liberation of Estonia from Nazi Germany. Following the relocation of the statue, the Russian government expressed its dissatisfaction. The Russian response came in the form of a series of cyber-operations against various Estonian targets, including political parties, ministries, Estonian government banks, media outlets and other targets, which were not critical but still resulted in the disruption of services, operations and communications. Some experts divided the cyber-attacks into three waves, while others divided them into four, and these included DDoS assaults and SQL injections that caused websites to go down entirely or partially. However, Russia did not achieve its desired goals, despite extending its cyber-attacks over several weeks. The allies and international community offered support to Estonia while Russia refused to cooperate in the investigation and vehemently denied any state-level implication. The cyber-attacks in the spring of 2007 were something of a turning point. Russia showed that it was willing and able to carry out hybrid actions, while Estonia became the first country to face a massive and surprising cyber-attack. Its capital Tallinn soon became the destination for NATO's Cooperative Cyber Defense Centre of Excellence (CCD CoE). (Polyakova, et al. 2020, 21)

In the 2008 Russo-Georgian War, both sides resorted to kinetic (conventional military strikes and troop movements) and non-kinetic offensive means (cyber-attacks, propaganda, denial and deception). This is the first real-world battle in which cyber-attacks and military operations have been combined. Such attacks have included website defamation, and distributed denial of service attacks against the Georgian government, Georgian media and financial institutions. The attacks succeeded in denying citizens access to 54 websites related to communications, finance and government. Russia has also engaged in intelligence-espionage operations including propaganda, information control and disinformation campaigns with varying results, particularly in contrast to Georgia's efforts in the same areas. Using television footage and daily interviews with a military spokesman, Russia controlled the international flow of information and attempted to influence local populations by dictating news, sharing the progress of Russian troops protecting Russian citizens, and highlighting Georgian atrocities. (Iasiello 2017, 2) Many of the techniques used against Estonia were used a year later against Georgia. If one looks at all aspects of the geopolitical situation, the timing of the attack and the relationship between the government and the youth groups that helped with the attacks, it is easy to conclude that Moscow was behind them. (Smith 2014)

The later protests in 2011-2013 over Russia's controversial elections demonstrated how the media can be used to generate waves of public discontent. These and the Arab Spring uprising already demonstrate the effectiveness of social media in regime change. What's more, they helped the Kremlin government develop information campaign capabilities that facilitated the annexation of Crimea in 2014.

Although there is no evidence of cyber actors within the Russian military who may have been involved in cyberspace activities, the insinuations indicate that Russia has learned from past mistakes. For example, the timing of cyber-attacks was considered the first strike for maximum effectiveness, especially on important targets such as critical infrastructure. Cyber-attacks against Crimea shut down telecommunications, disabled major Ukrainian websites and blocked the mobile phones of key Ukrainian officials before Russian forces entered the peninsula. (Iasiello 2017, 54) Many military experts said the cyber-attacks were undoubtedly executed to isolate Crimea and facilitate kinetic operations. The strategy on which the non-kinetic operations were based was propaganda, disinformation, denial, and deception to influence the domestic, regional and global situation.

The Kremlin's involvement in the ensuing elections for a referendum in which the Crimean parliament voted to join Russia was obvious. In general, elections are particularly vulnerable because they provide an opportunity for external actors not only to support a favorable candidate but also to sow doubts about the freedom and fairness of the elections. They can raise questions about the stability of the country and erode confidence in the democratic process. Russian interference has been identified in elections in several countries. The interference in the 2016 US presidential election is the most documented case showing Russia's *modus operandi* in using both information-technical and information-psychological tools. This took the form of acquiring and subsequently disclosing information on party documents, as well as personal data along with emails of candidates. However, targeted information and cyber operations were also observed in connection with elections in Ukraine, France, Sweden, the European Parliament and other countries. These are characterized by spear-phishing campaigns to access data, hacking operations and information leaks, disruptive attacks on electoral infrastructure and the use of the online environment for manipulation and spreading disinformation. (Hakala and Melnychuk 2021, 26)

Russia was involved or attempted to be involved including in the 2020 election, targeting more than 200 organizations including political parties and consultancies, according to Microsoft. The US National Intelligence Council declassified a document on the 2020 election showing that it would have been difficult for an outside actor to compromise the election, but that actions to compromise local and government networks were identified. Foreign actors such as Russia and Iran spread false or distorted information about the voting system to undermine public confidence in the electoral process. (Assesment 2021, 1-2) According to the same report, President Putin also allegedly authorized operations against the presidential election to denigrate Joe Biden and his party and to support President Trump by undermining public confidence in the voting process. Unlike the 2016 election, no sustained Russian cyber efforts to compromise the election infrastructure have been detected.

In the meantime, Russia's cyber infrastructure has been steadily developing, and so have the actors who specialize in cyber actions, so they have put together a broad hybrid action launched in February 2022 against Ukraine. A series of DDoS attacks against Ukrainian banking, government and defense websites were launched at the beginning of February and were allegedly launched by the Russian military intelligence agency (GRU). The attacks came amid heightened tensions between Ukraine and Russia. Despite the fact that many outside observers had expected a massive Russian cyber-attack before the conflict, it happened on a significantly lower scale. Moreover, Ukraine's strategy of mobilizing cyber specialists to defend itself and take offensive action against the Russians has had an effect. We can state, however, that the non-kinetic support of the military special operation was visible. Cyber-attacks from Russia continued to intensify in late March, mostly through attempts to gather intelligence and spread malware to Ukrainian critical infrastructure, according to a Ukrainian cyber official. Victor Zhora, deputy head of Ukraine's State Service for Special Communications and Information Protection, said the same group of Russian-linked hackers that targeted local Ukrainian government agencies with compromised emails also sent malicious emails to Latvian authorities. Between 23 and 29 March, 65 cyber-attacks took place on Ukraine's critical infrastructure, five times more than the previous week, targeting state and local authorities, Ukraine's security and defense sector, financial, telecoms and energy companies. (Stupp 2022)

Russian officials have said that countries that help Ukraine in this confrontation will face consequences. Indeed, a number of European countries have faced a series of threats from the cyber environment. Romania, a neighboring country of Ukraine, has faced a wave of DDoS cyber-attacks targeting several institutions, including the government, the Ministry of National Defense, the Border Police and the Romanian Railways website. The attacks were claimed by pro-Russian Killnet hackers. Apart from the fact that the websites of these agencies were down for a short period of time, there was no significant damage.

Such cyber-attacks on NATO member states should bring member countries together for consultations. By recognizing cyberspace as an operational area in 2016, NATO accepted its approach as a confrontational environment and prompted member states to reassess the cybersecurity domain, to make efforts in technological development to at least deter attempted cyber-attacks. Given the defensive nature of the Alliance and the need to deter cyber-attack attempts, the adoption of a coherent and adapted legislative framework at the international and local level could enable states that espouse defensive military doctrines to build reactive cyber defense strategies. Moreover, now is the time for the alliance to set the conditions for activating Article 5 NATO response: *"An attack on one ally will trigger a response from the whole alliance".*

Conclusions

The lack of international harmonization of cyber terms can create misunderstandings. One state's interpretation of cyber warfare terms may differ from another state's interpretation due to cultural or organizational differences.

It has a significant number of strategies, doctrines, laws, and regulations that are harmonized and updated frequently, which leads us to believe that it is very interested in the information phenomenon. It is no coincidence that Russia was one of the first countries to develop an information environment strategy.

In order to understand the purpose, directions, techniques, and procedures that the Russian Federation applies in the cyber environment, we have briefly reviewed some of the rules governing this area. In order to comprehensively edify the strategies and techniques used, we analyzed a number of activities attributed to or recognized by the Kremlin government. The first conclusion is that in fact, exactly these rules written by the Russian information think tank have been put into practice.

From the presentation of a number of cyber activities in the information environment for which Russia has been responsible, we learn that Russia has been very active since peacetime. Moreover, it takes the cyber offensive in international relations very seriously.

Another conclusion that emerges from what has been presented is the synergistic use of conventional and non-conventional actions in Russian hybrid warfare, with actions in the information environment supporting conventional military operations. It is no coincidence that Russia has a relatively large amount of government agencies responsible for the information space and controls a number of non-state actors.

Like any country, it finds it difficult to keep up with new technological challenges. The lack of communications and information technology and the desire to remain a secure and resilient state has led to the idea of abandoning the global internet and developing its own internet network. Moreover, even though the rules governing the information space mention free and equal access to information as a matter of fact, in reality, the sources of information are controlled by the state and personal data, information about the individual and conversations are stored for a period of time by telecommunications service providers. However, recent conflicts show that Russia does not hesitate to pursue its strategic goals whether internal, regional or global, and does not give up its aspiration to maintain its great power status.

Russia's most significant and recent cyber actions are those against Ukraine executed in support of its ongoing special military operation. The fact that a number of other states either in the region or NATO members have been targeted by some cyber-attacks is concerning. Against this backdrop, it is inherent to strengthen the international community's cyber defense and security against such operations, and through effective and credible diplomatic means to deter cyber. It is also an opportunity to show that NATO is a strong alliance and that it could activate Article 5 even in the event of a cyber-attack against a member country.

Bibliography

Assesment, Intelligence Comunity. 2021. "Foreign Threats to the 2020 US Federal Elections." *Foreign Threats to the 2020 US Federal Elections.* National Intelligence Council, 10 March.

Barry, Buzan, Wæver Ole, and Wilde Jaap. 1997. *Security. A New Framework for Analysis.* London: Lynne Rienner Publishers.

Blank, Stephen. 2017. "Cyber War and Information War à la Russe." In *Understanding Cyber Conflict: Fourteen Analogies*, by George Perkovich and Ariel E. Levite, 309. Georgetown University Press.

Bussell, Jennifer. 2013. *Encyclopedia Britannica.* 12 March. Accessed February 24, 2022. https://www.britannica.com/topic/cyberspace.

Clark, Mason. *Russian hybrid warfare military learning and the future of war series.* Washington, DC: Institute for the Study of War.

Defence, Russian Ministry of. 2011. "Conceptual Views on the Activities of the Russian Federation Armed Forces in the Information Space." Moscow: Russian Ministry of Defence.

Giles, Keir. 2012. "Russia's Public Stance on Cyberspace Issues." *4th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications. 63-75.

Godwin, James B., Andrey Kulpin, Karl Frederick Rauscher, and Valery Yaschenko. 2014. *Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2.* policy report, New York, Moscow: EastWest Institute and the Information Security Institute of Moscow State University.

Government, United States. 2018. *Joint Publication 3-12, Cyberspace Operations.* Scotts Valley, California: Createspace Independent Publishing Platform.

Hakala, Janne, and Jazlyn Melnychuk. 2021. *Russia's strategy in cyberspace.* Riga: NATO Strategic Communications Centre of Excellence.

Iasiello, Emilio J. 2017. "Russia's Improved Information Operations: From Georgia to Crimea." *Innovations in Warfare & Strategy.*

information, Russia's official state website for legal. 2017. *https://meduza.io/.* 10 May. Accessed May 21, 2022. http://publication.pravo.gov.ru/Document/View/0001201705100002?index=0&rangeSize=1

Jasper, Scott. 2020. *Russian cyber operations Coding The Boundaries Of Conflict.* Washington, Dc: Georgetown University Press.

Kukkola, Juka. 2020. "Digital Soviet Union The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas." *Digital Soviet Union The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas.* Helsinky: Finnish National Defence University, 27 May.

Latukhinamaxim, Kira, and Makarychev. 2013. *Russia beyond.* 25 FEB. Accessed May 20, 2022. https://www.rbth.com/international/2013/02/25/russia_updates_its_foreign_policy_concept_23211.html.

Lilly, Bilyana, and Joe Cheravitch. 2020. "The Past, Present, and Future of Russia's Cyber Strategy and Forces." *12th International Conference on Cyber Conflict.* Tallinn: NATO CCDCOE Publications. 129-155.

2017. *North Atlantic Treaty Organisation.* 29 March. Accessed January 23, 2022. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Polyakova, Alina, Mathieu Boulègue, Kateryna Zarembo, Sergiy Solodkyy, Kalev Stoicescu, Precious N Chatterje-Doody, and Oscar Jonsson. *The Evolution of Russian Hybrid Warfare.* Washington, DC: Center for European Policy Analysis

Presidential, Russian. 2000. "The Military Doctrine of the Russian Federation." Moscow, February 5.

Putin, Vladimir. 2018. *Committee on the International Affairs of the State Duma.* 12 August. Accessed May 21, 2022. https://interkomitet.com/foreign-policy/basic-documents/strategy-of-information-society-development-in-russia-until-2030/

Pynnöniemi, Katri, and Martti J. Kari. 2016. "www.*fiia.fi." www.fiia.fi.* December. Accessed May 20, 2022. https://www.fiia.fi/wp-content/uploads/2017/04/comment26_russia_s_new_information_security_doctrine.pdf

Robinson, Paul. 2010. *Dictionary of international security.* Cluj-Napoca: CA-Publishing.

Russian Federation, The Ministry of Foreign Affairs of the. 2016. "Foreign Policy Concept of the Russian Federation." *Foreign Policy Concept of the Russian Federation.* Moscow: The Ministry of Foreign Affairs of the Russian Federation, 30 November. https://www.rusemb.org.uk/rp_insight/

Smith, David J. 2014. *Atlantic Council.* 17 January. Accessed May 20, 2022. https://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia/

Stupp, Catherine. 2022. *wsjpro cybersecurity.* 5 April. Accessed May 21, 2022. https://www.wsj.com/articles/russian-cyberattacks-increase-on-ukraines-critical-infrastructure-report-11649186873

Timur Chabuk, Adam Jonas. 2018. *AFCEA.* 1 September. Accessed May 17, 2022. https://www.afcea.org/content/understanding-russian-information-operations.