e-ISSN: 2687-3583
https://dergipark.org.tr/trad

TRAD - Türkiye Rusya Araştırmaları Dergisi 3 (Yaz 2020)

TJORS - Turkish Journal of Russian Studies 3 (Summer 2020)

Başlık / Title: Analysis of Russia's Cyber Security and Cyber Espionage Policies

Yazarlar / Authors **ORCID ID**
Hasan ACAR 0000-0001-8956-7836
Mustafa PEKCANDANOĞLU 0000-0002-1776-6673

Bu makaleye atıf için: Hasan Acar ve Mustafa Pekcandanoğlu, Analysis of Russia's Cyber Security and Cyber Espionage Policies, *Türkiye Rusya Araştırmaları Dergisi* 3 (2020): 167-189.

To cite this article: Hasan Acar ve Mustafa Pekcandanoğlu, Analysis of Russia's Cyber Security and Cyber Espionage Policies, *Türkiye Rusya Araştırmaları Dergisi* 3 (2020): 166-188.

Makale Türü / Type of Article: Araştırma Makalesi / Research Article
Yayın Geliş Tarihi / Submission Date: 29.05.2020
Yayına Kabul Tarihi / Acceptance Date: 29.06.2020
Yayın Tarihi / Date Published: 30.06.2020

Tarandığı İndeksler Abstracting & Indexing

Yazar: Hasan ACAR[*]
Mustafa PEKCANDANOĞLU[**]

Rusya'nın Siber Güvenlik ve Siber Espiyonaj Politikalarının Analizi

Öz: Ulusal güvenlik politikaları, son yıllarda küreselleşmenin getirdiği sonuçlarla birlikte daha kırılgan bir yapıya kavuşmuştur. Devletler günümüzde sınır güvenliğinden ziyade bilgi ve teknoloji güvenliğine önem vermeye başlamıştır. Siber güvenlik kavramı bu noktada son yıllarda gelişen güvenlik alanlarından birini oluşturmaktadır. Teknolojinin akıl almaz hızı karşısında, güvenliğin sağlanması her geçen gün zorlaşmaktadır. Bu nedenle devletler siber güvenlik alanında sürekli kendi tedbirlerini güncellemek durumunda kalmışlardır. Bunun yanında devletlerarası ilişkilerde siber güvenlik alanı, sürekli devam eden bir bayrak yarışını andırmaktadır. I. Dünya Savaşı öncesinde başlayan silahlanma yarışına benzer bir şekilde, siber güvenlik alanında devletlerarasındaki rekabet devam etmektedir. Bu rekabet içerisinde etkin olarak varlık gösteren devletlerden biri kuşkusuz Rusya'dır. Rusya'da 2000'li yıllarla birlikte bir devlet politikası haline gelen siber güvenlik alanı, günümüzde de gelişimini sürdürmektedir. Amerika Birleşik Devletleri (ABD)'nde 2016 Başkanlık seçimleriyle yeniden gündeme gelen siber güvenlik kavramı, günümüzde ve gelecek yıllarda güvenlik politikaları içerisindeki etkin varlığını sürdürecektir. Siber güvenlik kavramı genelde akıllara orduları ve istihbarat örgütlerini getirmiştir. Rusya ise ordu ve istihbarat faaliyetlerinde siber hâkimiyetini güçlendirmesinin yanında diğer tüm alanlarda da bu teknolojiyi kullanmaya çalışmış ve vatandaşlarının bilgi kaynaklarını kontrol altında tutmak istemiştir. Rusya siber güvenlik alanındaki bu faaliyetlerini sadece belirli devlet kurumları ile sınırlandırmamıştır. Devlet kontrolünde bulunan fakat devletin herhangi bir kurumuna bağlı olmayan hacker grupları ile siber güvenlik faaliyetleri desteklenmektedir. Bu makale, bahsedilen bu bilgiler ışığında Rusya'nın siber güvenlik ve siber espiyonaj politikalarını analiz etme amacı taşımaktadır. Bu kapsamda makalede, Rusya'nın siber güvenlik faaliyetlerinin gelişimi tarihsel bir süreçle ele alınacak ve Rusya'da siber güvenlik alanında faaliyet gösteren devlet ve devlet dışı aktörler ortaya koyularak Rusya'nın siber güvenlik kapasitesi analiz edilecektir.

Anahtar Kelimeler: Uluslararası Güvenlik, Güvenlik Politikaları, Siber Güvenlik, Siber Espiyonaj, Rusya.

Analysis of Russia's Cyber Security and Cyber Espionage Policies

Abstract: National security policies have attained a more fragile structure with the results of globalization in recent years. States have started to give importance to information and technology security rather than border security today. The concept of cyber security is one of the security areas that have developed in recent years at this point. In the face of the incredible speed of technology, it becomes more difficult to ensure security day by day. For this reason, states had to constantly update their measures in the field of cyber security. Besides the field of cyber security in interstate relations resembles an ongoing flag race. Similar to the arms race that started before the First World War, interstate competition continues in the field of cyber

[*] Ph.D., Gendarmerie and Coast Guard Academy, Bursa/Turkey, E-mail: hasanacar.uludag@gmail.com, ORCID ID: 0000-0001-8956-7836.
[**] Master Student, Marmara University, Faculty of Business Administration, Istanbul/Turkey, E-mail: mustafapekcandanoglu@marun.edu.tr, ORCID ID: 0000-0002-1776-6673.

security. Undoubtedly, Russia is one of the states that actively exist in this competition. The cyber security field, which has become a state policy in the 2000s in Russia, continues its development today. The concept of cyber security, which came to the agenda again with the 2016 Presidential elections in the United States of America (USA), will continue its effective presence in security policies today and in the coming years. The concept of cyber security generally brought to minds and intelligence organizations. Russia, on the other hand, tried to use this technology in all other areas as well as strengthening its cyber domination in military and intelligence activities and wanted to control the information resources of its citizens. Russia has not limited its activities in the field of cyber security to certain state institutions only. Cyber security activities are supported by hacker groups under state control but not affiliated with any government agency. This article aims to analyze Russia's cyber security and cyber espionage policies in light of this information. In this context, the development of Russia's cyber security activities has been handled with a historical process and the cyber security capacity of Russia has been analyzed by revealing state and non-state actors operating in the field of cyber security in Russia.

Keywords: International Security, Security Policies, Cyber Security, Cyber Espionage, Russia.

Introduction

States have a responsibility to ensure the security of their citizens. The needs of security policies change over time. Technology has emerged as a very important factor in this change. In line with efforts towards digitalization, people's daily routines are progressing through digital media as well as storing data electronically. The technological devices used are spread over a wide part of our daily life. This situation, which facilitates the daily life of people, can cause negative consequences if necessary measures are not taken in terms of security. In this context, it is not possible to ignore this situation while creating today's security policies.

All activities carried out in the digital environment occur in cyber space. Cyber security policies are developed to ensure security in cyber space. Cyber security policies are not only limited to defense purposes but also used for attack purposes. States that have developed policies in the field of cyber security have provided an advantage in security policies. Russia, which has developed very effective policies in the field of cyber security, has taken the lead with several countries in the world. In addition to this, Russia has been exposed to attacks in the field of information security and has been damaged. Russia, which produces intense activities to reverse this situation, continues to increase its investments in this field today.

In addition to intensely developing cyber security policies to ensure its internal security, Russia has benefited from this area in line with the interests in its foreign policy. This situation, which contains many examples,

has increased the importance given to the field by the Russians and paved the way for larger investments in this field in the future.

Many state institutions in Russia that have responsibilities in the field of cyber security. A detailed examination of the duties of these institutions will lead to an understanding of Russia's cyber security strategy in the future. Also Russia has hacker groups working in the interests of Russia in addition to its official power in cyber space. Russia foresees that these groups may be harmful in some cases besides their useful services. For this reason and with intending to increase control over its citizens, it continued its activities on a strategy aimed at centralizing the cyber domination of Russia, which includes local administrations, private companies and some educational institutions. With these developments in the field of cyber security, Russia has aimed at its competitive advantage in many fields, especially in security, compared to other countries.

Conceptual Analysis

Many definitions have been made to explain the concept of cyber security. In summary, cyber security is the protection of cyber systems against potential threats. The advancement of technological developments with great momentum has caused the digitalization trend of the existing systems. Technology facilitates daily life, causes cost advantage, processing data and making improvements on the system. For reasons, digitalization has continued rapidly. The digitalization of systems has reached a point that spreads not only with large projects but also throughout the society. For example, it may be that a farmer engaged in agriculture controls the irrigation system on the phone for the best growth of the crop, or banks serve their customers with mobile banking applications. Even looking at these two examples, it can be seen that the extent to which the cyberspace spans, as well as its importance. Besides today's age is referred to as the "data age".[1]

All digital devices, such as mobile phones, computers, smartwatches, televisions, or even white goods, collect data. In this context, our fridge may know of our eating habits, smartwatches up to our heartbeat, and televisions know about the programs we like. Mobile phones and computers keep our messages and emails in addition to our personal information. As these technological devices overlap the human data, the necessity of the careful

[1] McKinsey Global Institute, "The Age of Analytics: Competıng in a Data-Driven World", Executive Summary, December 2016, Access: 28.05.2020, https://www.alvaroriascos.com/mineriadatos/The-age-of-analytics-Executive-summary.pdf.

protection of the information here has been revealed. In addition to the need for personal protection, the need to protect states, the business world, and many other areas have also emerged. Because the cyber attack of a digital system can cause great damage. For example, a cyber attack on a fully digital factory can cause all production to stop or disrupt a bank's transactions or even disrupt the services of government agencies. States and the private sector have worked to ensure cyber security. Apart from protecting information and systems, cyber security is emerging as a new battlefield.

Historical Background

Russia, as a successor of the USSR, has a technological background from the past. Due to this technological knowledge, Russia has developed solutions to the problems it faces. Russia's development of cyber security strategies can evaluate in this context. This strategy is expressed as an information security policy rather than a cyber security policy. The production of policies related to the concept of information security emerged with the 1994 Russian-Chechen War. This war ended in a severe defeat for Russia. Although Russia intervened in Chechnya with a strong military force, it failed. The Chechnya War has ceased to be an internal problem of Russia and a situation that has made a global impact has emerged. The situation in Chechnya was much more than a traditional war. Chechens used information technologies very well in this war. Important reactions have been received from the West to Russia's intervention in Chechens. It was argued by the West that human rights are a product of the international community and that Chechen people have the right to self-determination.[2] Chechnya people, besides reflecting the persecution of the Russians very well, had an impact on the Russian public opinion. The Russians realized this situation and made a rapid change in their war strategies.[3] Russia has brought the production of the information under control and reflected the war here to the world public as it intended. Russia wanted to break the popularity of this war, which gained tremendous popularity. Instead, Russia wanted to reflect the image of a simple military operation there. In line with these policies, Russia put great pressure on the media. Media organizations are taken into government control and adjustments were made in the local press accreditation system.

[2] Cevher Sunçkale, *Çeçen Savaşı* (Ankara: Sam Yayınları, 1995), 103.

[3] See more: Senem Öztürk, "Jeopolitiğin Rusya Federasyonu'na Etkilerinin Kuzey Kafkasya-Gürcistan Güney Osetya Çerçevesinde İncelenmesi", *Güvenlik Stratejileri*, 9/17 (2013): 201-242.

With the experience of Chechnya, Russia has realized the vital importance of the concept of information security. After this experience, Russia has developed policies to increase information security and control over cyber space. The Russians noticed this critical area years ago and made investments on it. Officially, the information security doctrine called *"National Security Concept of the Russian Federation"*, which was the first of its kind, declared in 2000 during the time of Russian President Vladimir Putin. This doctrine has become the guide book of Russian cyber security policies. Also Russia did not just take an approach to media domination. Russia has addressed cyber power not only within its borders but also as an international power field. Russians have made efforts to adapt their institutions to this transformation process.[4]

The first main document on the way of Russia's goal of becoming cyber power is accepted as *"Information Security Doctrine of the Russian Federation"* published on September 9, 2000. This doctrine outlines Russia's principles, objectives and official views on information security. *"Russia's National Security Strategy to 2020"* dated May 12, 2009, is remarkable in that it is fully security-oriented. This strategy document was an essential official document for the Russian security and intelligence services at the time of its adoption and was an important official document. The document published in 2011 called *"Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space"*, on the other hand, it can be defined as "the preliminary cyber war doctrine of the Russian Army". In this context, it can be argued that the document is the first clear text to accept Russian military presence and mobility in cyber space. Unlike other Russian documents, this document was written from a perspective that centered information. Valery Gerasimov, who was appointed as the Russian General Staff in 2012, in his article "The Value of Science in Prediction", the military approach was defined as the *"Gerasimov Doctrine"*. Russia, non-military methods, within the principles expressed by the Gerasimov Doctrine, with conventional power aimed to direct it to conflict processes. *"Concept of the Foreign Policy of the Russian Federation"*was approved in February 2013 with the approval of Russian President Vladimir Putin. In this document, which deals mainly with the future goals and principles of Russia's foreign policy, there are some determinations and evaluations regarding information and cyber security. With the *"Basic Principles for State Policy of the Russian*

[4] Andrei Soldatov and Irina Borogan, "Russia's approach to cyber: the best defence is a good offence", *Hacks, Leaks and Disruptions Russian Cyber Strategies*, Eds. Nicu Popescu and Stanislav Secrieru (Paris: European Union Institute for Security Studies, 2018), 15-17.

*Federation in the Field of International Information Security" r*eleased in 2013, the foundation in Russia's international information security field elements have been identified.[5]

As a result of all these developments, a doctrine was published containing past experiences. The document *"Doctrine of Information Security of the Russian Federation"* published on December 5, 2016, has become a comprehensive document on Russia's information security policy. The concept of information security is underlined in the document. It is understood from the subheadings that this doctrine is a doctrine based on the concept of information security. This doctrine consists of five parts. These are: *"General Provisions, National Interests in the Information Sphere, Major Information Threats, Strategic Objectives and Key Areas, Institutional Framework of Information Security."*[6]

A more detailed consideration of the concept of information security on the doctrine will provide a better understanding of Russia's perspective on this issue. There are differences between Russia and Western countries in terms of handling the concept of cyber security. The Western world has used the concept of cyber security with a more technological approach. In contrast, Russia and China used the concept of information security.[7] These two different words not only made a difference in terms of use. Russia's approach to the concept of information security has shown that it holds control at a wider level. Because while the USA and Europe regard cyber security as ensuring the security of the infrastructure, Russia wanted to keep the information control together with the security of the infrastructure.[8]

Looking at these two different situations, it was seen that Russia took a more authoritative approach. The following statements in the doctrine can be evaluated in this context:

---

[5] Ali Burak Darıcılı ve Barış Özdal, "Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi", *Ahmet Yesevi Üniversitesi Türk Dünyası Sosyal Bilimler Dergisi (BİLİG)*, Avrasya'nın Siyasal İktisadı Özel Sayısı (2017): 124-125.

[6] The Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation*, Approved by Decree of the President of the Russian Federation, No. 646 of December 5, 2016.

[7] Emilio Iasiello, "Russia and China Are Making their Information Security Case", *The Cyber Research Data Bank*, Access: 28.05.2020, https://www.cyberdb.co/russia-and-china-are-making-their-information-security-case/.

[8] Pasha Sharikov, "Understanding the Russian Approach to Information Security", *European Leadership Network*, Access: 28.05.2020,
https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/, January 16, 2018.

"Intelligence services of certain States are increasingly using information and psychological tools with a view to destabilizing the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of other States. Religious, ethnic, human rights organizations and other organizations, as well as separate groups of people, are involved in these activities and information technologies are extensively used towards this end. There is a trend among foreign media to publish an increasing number of materials containing biased assessments of State policy of the Russian Federation. Russian mass media often face blatant discrimination abroad, and Russian journalists are prevented from performing their professional duties. There is a growing information pressure on the population of Russia, primarily on the Russian youth, with the aim to erode Russian traditional spiritual and moral values. "[9]

Russia has foreseen that with the spread of unhealthy information within the borders of the country, different ethnic groups in the country can rise with a revolt or that these groups can form armed terrorist organizations.

Although the reason for the outbreak of the Russian-Chechen War was not only due to the lack of information security, what happened during the war revealed that the anxiety about information security was not unfounded. Russia was concerned about the possibility that the information technologies owned by the West could be used against itself. For this reason, Russia wanted to increase the nationalization rate of cyber security elements in terms of hardware and software to ensure information security.[10]

Russia wanted to protect and expand its dominance in cyber space with these steps taken. Russia also wanted to switch from a scattered cyber structure that creates image loss to itself to a more regular cyber security system structure and not to limit cyber security efforts not only to the central government but also to include local governments in its field in cyber space. In this way, the more organized defense is envisaged against both domestic security and an attack focused abroad. Russia wanted to keep its citizens' access to information under control. In a country with authoritarian tendencies like Russia, the effort of keeping citizens under control in terms of information source has been vital for regime continuity. In this published doctrine, it has been stated that cyber attacks, military and political purposes, as well as Russia's economic security, must be provided. In this context, the statements in the doctrine are as follows: *"There is a rise in*

[9] The Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation.*

[10] Iasiello, "Russia and China Are Making their Information Security Case".

computer crimes, primarily in credit and financial sphere. The number of crimes related to violation of constitutional, human and civil rights and freedoms, including with respect to privacy, personal and family life, in the processing of personal data with the use of information technologies, is also increasing. The methods, means and tools used to commit such crimes get more and more sophisticated."[11]

Nowadays, the necessity of cyber protection of the economic system, which forms the sensitive side of the countries, has emerged. Unlike the organized cyber security organization of countries, even hackers who work irregularly can cause great damage to banks and financial institutions. Besides even if there is no robbery, even the locking of the transactions of any bank for a certain period time can cause great losses. It has not been possible to protect cyber security only through policies to be taken by states. At this point, it is predicted that a total defense model will produce more successful results. With the strategies it has developed, Russia has aimed to contribute to the cyber space domination of both local governments and private organizations. Russia has increased its power in this field with the policies it has developed in the field of cyber security. However, at the point reached, the perception of Russia intervening in the internal affairs of the states through cyber attacks has occurred. Although it has not been proven, many events have been claimed that Russia has an impact. It was alleged that Russia played a role in Donald Trump's election by intervening in the 2016 presidential elections that made the most speech.[12] This situation has caused great repercussions all over the world, especially in the USA. The fact that Russia gives such an image has been evaluated that it may pose new problems in the coming years. By evaluating such a risk, Russia wanted to make its cyber power more centralized and controllable. Despite all the negativities, from a historical point of view, Russia has strengthened its domination in cyber space. Russia continues to develop its cyber power, strives for progress and gains in cyber security policies by making the necessary reforms.

Russia's Cyber Security and Cyber Espionage Strategy

Russia has many state institutions that have a responsibility in cyber security policy. The officially recognized institutions responsible for the

[11] The Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation.*

[12] BBC News, "Trump Rusya'nın ABD seçimlerine müdahale ettiğini kabul etti", July 17, 2018, Access: 28.05.2020, https://www.bbc.com/turkce/haberler-dunya-44866605.

implementation of a national cyber security strategy, policy and roadmap in Russia are:

- *Russian Federal Security Service (FSB),*
- *Federal Protection Service (FSO),*
- *Federal Service for Technical and Export Control (FSTEC),*
- *Ministry of Internal Affairs (MVD),*
- *Ministry of Defence (MoD)*
- *Foreign Intelligence Service (SVR)*

In addition, some of the functions are carried out by Federal Law 152 on Personal Data Protection -regulated by Roscomnadzor- (Telecommunications Regulator).[13]

Among these, the Russian Federal Security Service (FSB) has gained an important place among the institutions that have responsibilities in Russia's cyber security policies. FSB was established as the agency responsible for internal intelligence after the abolition of the Committee for State Security (KGB: *Komitet Gosudarstvennoy Bezopasnosti*). After its establishment, the impact of former KGB employees on FSB continued. In the period of Russian President Boris Yeltsin, the responsibilities given to the FSB were expanded. During Vladimir Putin's presidency, his duties abroad were added to his duties at home. The FSB made important contributions in suppressing the Chechen rebellion. The FSB has been a highly influential institution in counterintelligence.[14]

Another government agency responsible for information security policy was the Federal Protection Service (FSO: Federal'yaya Sluzhba Okhrani). The foundation purpose of FSO was not focused on ensuring information security. FSO has begun to be effective in information security policies with innovations within the organization in the changing world with the effect of technological developments. As a result of the main duties undertaken by the FSO, it has become a country with significant influence. These tasks were mainly to supervise the communication of top-level bureaucrats, to operate underground command centers, to ensure certain areas of strategic importance and the transport security of high-level bureaucrats. The institution, which is named FSO today, carried out its activities under the name of Russia Main Guard Directorate (GUO) until 1996. FSO received

[13] ITU, "Cyberwellness Profile Russian Federation", *Global Cybersecurity Index & Cyberwellness Profiles*, (2015): 389-391, Access: 28.05.2020, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

[14] Robert W. Pringle, "Federal Security Service: Russian Government Agency", *Britannica*, Access: 28.05.2020, https://www.britannica.com/topic/Federal-Security-Service.

some of its duties in the field of information security from the authorizations made during the GUO period. In 1992, with the initiative of Mikhail Barsukov[15], the GUO was assigned to the presidential communication task carried out by the Federal Agency of Government Communications and Information (FAGCI / Russian: ФАПСИ: FAPSI: Federal'noe Agentstvo Pravitelstvennoi Svyazi I Informatsii). The communication task undertaken by FSO has been further expanded. In 2003, Special Communications and Information Service of the Federal Protective Service of the Russian Federation: Spetzzvyaz was established under the leadership of Kornev Yuri Pavlovich, who was working at FSO.[16]

On 7 August 2004, by the decision of President Vladimir Putin, Spetzzvyaz was organized as part of the FSO institution[17]. The duties of the Spetzzvyaz institution is a cryptological intelligence agency that undertakes the tasks of external communication, gathering external signal intelligence, analyzing this collected data, and protecting state communication and information systems.

Spetzzvyaz has become a key institution in terms of information security with its duties. Another institution that has responsibility in cyber security policies was the Federal Service for Technical and Export Control (FSTEC). FSTEC was established in 2004 as an organization affiliated to the Ministry of Defense of Russia. FSTEC's main task was to control information security and export of sensitive technology. FSTEC has the authority to license organizations and technologies. In addition, FSTEC conducts studies to protect the cyber security of information and telecommunication networks from foreign penetration. FSTEC shares laws and regulations on information security on its official website. On this site, institutions that have certificate qualifications about cyber security projects are shared.[18]

FSTEC investigates and projects information security threats and organizes training for its staff in line with the latest developments and

---

[15] *Russia National Security and Defence Policy Handbook: Vol 1 Strategic Information and Basic Laws* (Washington: International Business Publications, 2007), 278-279.

[16] Globalsecurity, Intelligence, "Federal Protective Service (FSO) Federal'naya Sluzhba Okhrani", https://www.globalsecurity.org/intell/world/russia/fso.htm, Accsess: 28.05.2020.

[17] Federal Service of Security of the Russian Federation, "Structure: Tasks and Powers of the Federal Security Service of Russia", http://fso.gov.ru/struct/zadachi_polnomochiya/, Accsess: 07.06.2020.

[18] FSTEC of Russia, Documents and Projects, Access: 28.05.2020, https://fstec.ru/normotvorcheskaya/proekty.

develops measures against possible threats. There is also a scientific research institute within FSTEC.[19]

FSTEC has benefited from this institute in researching new information security threats, producing projects and training activities in the light of the latest developments of its staff. FSTEC has shed light on other state institutions that have responsibilities in the field of cyber security. Finally, FSTEC's mandate has been expanded to monitor websites and social media content. The duties of the eighth chief communications officer and the sixteenth electronic intelligence directorate departments operating within the intelligence service KGB in the USSR period were reorganized under the Federal Agency of Government Communications and Information (FAPSI) after the USSR broke up. After FAPSI was abolished in 2003, the powers of Russian Federal Security Service (FSB: The Federal Security Service of the Russian Federation), The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU / GU: Glavnoye Razvedyvatel'noye Upravleniye) and Foreign Intelligence Service (SVR: Sluzhba vneshney razvedki Rossiyskoy Federatsii). The main activity of SVR, which is among these institutions, was to carry out Russian foreign intelligence responsibility. In addition, he has the tasks of collecting intelligence from strategic signal intelligence, wireless communications, military and commercial satellite systems, and analyzing them.[20]

SVR, which seems to have more limited cyber security responsibilities than FSB and GRU, has come to the fore in cyber operations especially in foreign countries by trying to improve its capacity in this field in recent years.[21] Another Russian intelligence agency that works in the field of foreign intelligence, such as SVR, is The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). GRU continues its activities under the Ministry of Defense of Russia and is the largest intelligence service in Russia. In cyber operations carried out by Russia, GRU came to the fore. GRU conducted in recent years has been the knowledge that the next war, Estonia, Georgia, Ukraine, Turkey and made cyber attacks on state institutions in the United States has alleged that the GRU share. Many Russian hackers work within GRU. The Russians,

---

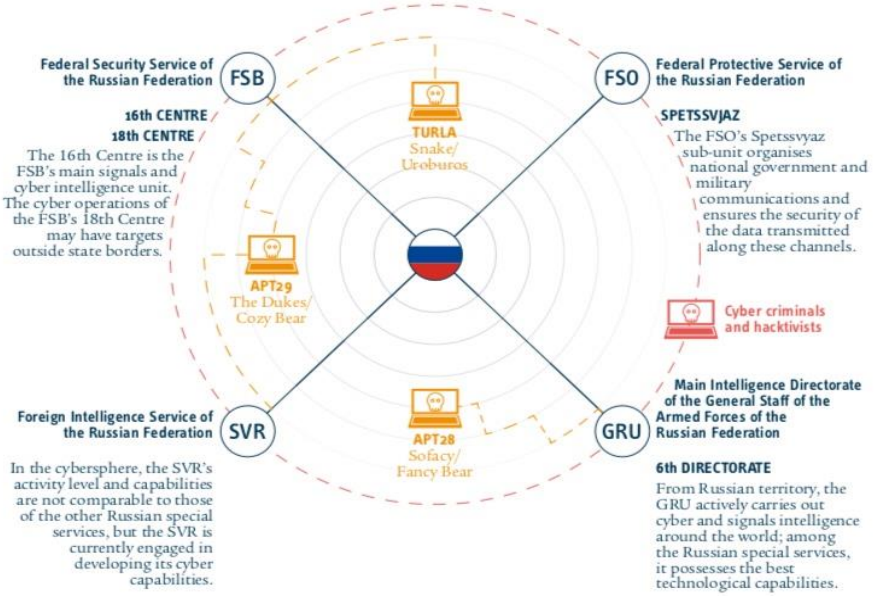
[19] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, (Sebastopol: O'Reilly Media, 2012), 225.

[20] Ruşen Eşref Yazgan, *Muhaberat Muhaberatı Bilgi Harbi Genel Değerlendirmeler ve ABD, Rusya Çin Örnekleri*, (2013): 113-114.

[21] Piret Pernik, "The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine", *Hacks, Leaks and Disruptions Russian Cyber Strategies*, Eds. Nicu Popescu and Stanislav Secrieru, (Paris: European Union Institute for Security Studies, 2018), 54.

especially due to their activities in recent years, have received great reactions from the world public opinion and aimed to increase their cyber attack capacity. A trainer at GRU's cyber training center stated that students are developing cyber attack algorithms to prepare for possible future cyber operations.[22]

Figure 1. Russia's Cyber Espionage Actors[23]



GRU has become an institution that has made a name for itself in recent years by keeping up with its deep-rooted historical background, strong corporate structure and the developments of the world today. Despite all the reactions received from the world public opinion with the operations and steps it has taken, it has tried to increase its institutional strength. In the activities carried out by the Federal Communication, Information Technology and Mass Communication Supervision Service (Roscomnadzor), ensuring the demand for society in high-quality telecommunication services as well as information and communication technologies, promoting the freedom of mass communication and mass media, protecting citizens' privacy, personal and family privacy rights. It intended. Roscomnadzor operates under the Ministry of Telecom and Mass Communication of the

[22] Cyber Security Intelligence, "What is the GRU & Who Does It Hack?", Uploaded on November 22, 2018, Access: 28.05.2020, https://www.cybersecurityintelligence.com/blog/what-is-the-gru-and-who-does-it-hack-3904.html.
[23] Pernik, "The Early Days of Cyberattacks", 54.

Russian Federation (Minsvyaz). There is a research and development center under Roscomnadzor. Roscomnadzor is an institution authorized to license and supervise in the fields of telecommunications, information technologies and mass communication. Informregistr, a research center affiliated to Roscomnadzor, examines the information security of Russia, conducts research and reports its results.[24] Russia, which wants to consolidate its power in the field of cyber security, has worked with hacker groups in addition to official state institutions. Although Russia does not want to accept these claims, there are strong signs of supporting some hacker groups.[25]

Russian hacker groups and their activities attracted the attention of the world public opinion. Working with hacker groups was not only an option the Russians preferred. Many states have applied this way to take advantage of the privacy provided by the gray area. In operations where hacker groups are used, it cannot be proved who operated. This has been an interesting situation for states. In addition, these groups, which are not employed like a regular army, were applied when needed, which led to an advantage in terms of cost. The sacrifices made by the nationalist hacker groups in terms of cost were also an advantage. In addition to the advantages of using these groups, they can also have disadvantages. The control of these groups, which lacked an institutional state structure, has been difficult in some cases. This situation coincides with a situation involving mercenaries. According to a regular army, the troubles seen in mercenaries who are undisciplined, rule-free and far behind in terms of military capability can also be seen in hired hacker groups. In addition, when nationalistic feelings were left aside, it was seen that individuals belonging to hacker groups could change sides for financial reasons. An individual who has worked for any state in the past can carry out activities against that state today. Besides, until he came to the hired hacker groups, he left the national army of the state to which he belonged and changed sides. In its report published in 2017, The New York Times transferred the Israeli 8,200 retired army personnel to DarkMatter, a cyber security company that has a close relationship with United Arab

[24] Roskomnadzor, "Statute of Roskomnadzor", Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (The Federal Service for Supervision of Communications, Information Technology, and Mass Media), Access: 28.05.2020, http://eng.rkn.gov.ru/about/.

[25] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare", *CNA Analysis & Solutions* (2017), 8.

Emirates intelligence. DarkMatter has hired people who previously served for the U.S. National Security Agency (NSA).[26]

The loss of personnel in the field of cyber security, where the states are competing with each other, caused a great disadvantage. Cyber security technologies developed as a result of large investments and efforts are in the hands of the competing country through the transfer personnel. This situation caused time, labor and money loss for the states. Looking at Russia's cyber security policy, it is aimed to gather cyber power in the center over the years. The increase in the cyber capacity of the Russians continued steadily. Organizations that can call the cyber army working directly for the state have been seen in Russia. These organizations continue their activities without interruption.

In this respect, the cyber attacks allegedly carried out against Estonia in 2007, Georgia and Lithuania in 2008, Kyrgyzstan in 2009, and finally Ukraine in 2014, have exhibited Russia's cyber attack capacity. It gives important clues about how it is used within the scope of the solution of policy problems. Because these attack allegations show how much Russia is using the new possibilities of cyber space within the scope of the solution of foreign policy problems.[27]

The Manas Military Base in Kyrgyzstan, which is carried out by the political interests of the Russian Federation, used the DDoS method as a common feature (Distributed Denial of Service Denial of Service) in Lithuanian attacks.[28] In this type of attack, it sends requests over its capacity for manipulation to the target network resource, thus preventing the network infrastructure from working in a healthily.[29] With this blocking, daily operations of the network infrastructure under attack are disrupted. The Russians used this type of attack precisely for this purpose. Thus, daily transactions in the target country are hampered and the citizens of the country under attack suffer damage. The main cyber attacks organized by the Russian Federation were against Estonia, Georgia and Ukraine. The Russian Federation attacked Estonia in 2008. The dispute between the two countries was moved to the cyber space. Estonia has become a country with

---

[26] Pınar Hilal Balta, "İsrailli istihbaratçılar BAE'li şirket için Tel Aviv'deki işinden ayrılıyor", *Timeturk*, October 17, 2019, Access: 28.05.2020, https://www.timeturk.com/israilli-istihbaratcilar-bae-li-sirket-icin-tel-aviv-deki-islerinden-ayriliyor/haber-1251495.

[27] Ali Burak Darıcılı, "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi", *U.U. International Journal of Social Inquiry* 7/2 (2014), 4-5.

[28] Darıcılı, "Rusya Federasyonu", 9-10.

[29] Kaspersky, "DDoS saldırısı nedir?", Access: 29.05.2020, https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks.

strong technological infrastructure and high digitization. Using this as an opportunity, the Russians attacked Estonia. The attack targeted the Estonian Parliament, Estonia's largest bank, websites of political parties, telecommunications companies.[30]

The attacks carried out succeeded, causing the services to be disrupted. In this process, Estonia received support from North Atlantic Treaty Organization (NATO) and the USA. After the attack, Estonia took measures for cyber defense and made investments. Another cyber attack was carried out on Georgia. The attack on Georgia was an example of hybrid warfare[31], as the different elements were carried out in cooperation. The Russian Federation both invaded Georgia with its military forces and made cyber attacks. The source of the problem between the two countries stemmed from Georgia's rapprochement with the west in recent years. Georgia carried out a military operation on Abkhazia and South Ossetia, which were virtually independent. In response, Russia launched a military operation on Georgia in response.[32]

Georgia, which has a much lower digitization rate than Estonia, has suffered relatively less from cyber attacks. Ukraine is one of the countries where Russia has carried out cyber attacks. With the Georgia case, tense relations emerged based on Ukraine's rapprochement with the EU turned into conflicts. Approaching this case with a hybrid war strategy, Russia also effectively used cyber security technologies. With the cyber activities it carried out, Russia provoked the people against the Ukrainian government in the regions where the Russians live densely. He wanted to fuel the fire of the rebellion that was caused by the false news spread by Russia by polluting information. With this operation, the cities of Donetsk and Lugansk fell into the hands of Russian rebels. Besides these cities, Russian militia was organized in a short time in Crimea. Another cyber operation of the Russians in Ukraine was for Crimea. The infrastructure of Ukrtelecom, the official mobile phone company of Ukraine, has been collapsed and the internet speed has been slowed down.[33]

For this purpose, it has been aimed to create a problem by serving the world in Crimea. When we look at the cyber capacity and cyber activities of Russia, it has been seen that the steps taken in the field of cyber security

[30] Connell and Vogler, "Russia's Approach to Cyber Warfare", 13.

[31] For detailed information on the hybrid warfare method, see more: Hasan Acar, "Küresel Terörün Uluslar arası Politikadaki Yeni Aktörü: Hibrit Savaş Modeli", *Küresel Terör ve Güvenlik Politikaları*, ed. Hasan Acar (Ankara: Nobel Akademik Yayıncılık, 2020), 57-71.

[32] Darıcılı, "Rusya Federasyonu", 7.

[33] See more at: Darıcılı, "Rusya Federasyonu".

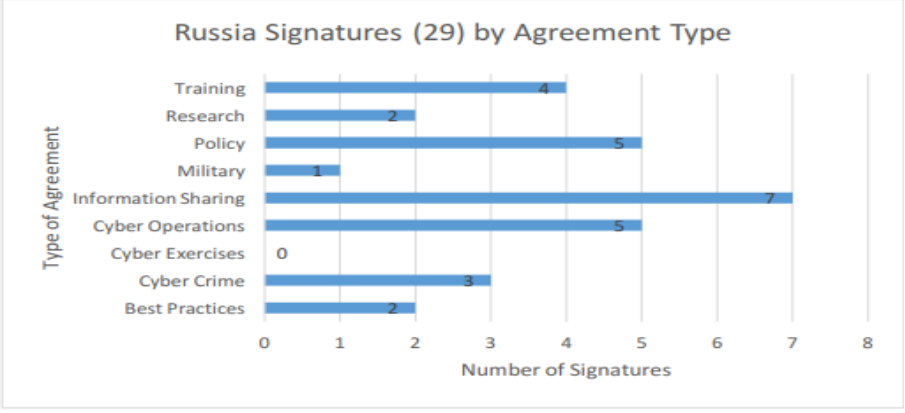
have also met in the field. Because when Russia included cyber power in addition to its current power, it was seen that it achieved significant gains. Russia has managed to quickly compensate for the experience of not being able to use the information war effectively.

In particular, the successful performance of GRU during the Ukrainian intervention of the Russian Armed Forces in 2014 is an example of the effective use of information technologies. Multi-dimensional hot combat performance called GRU's Gerasimov Doctrine or Hybrid War draws attention in the context of realizing this goal. At this point, the success of GRU emerged in manipulating the US Presidential Elections.[34]

Current Developments in Russian Cyber Policy

Examining the current developments of Russia in the field of cyber security through bilateral, regional and international agreements will shed light on the understanding of Russia's future strategy in this field.

Figure 2. Classification of Agreements in Russia's Cyber Security Area[35]



While Russia has been using cyber security technologies, it has not built it solely on its strategy to protect data or systems. Russia has attached special importance to the concept of information security, which it emphasizes in the official documents it publishes. Russia wanted to tightly control the information security of its citizens with cyber security

[34] Ali Burak Darıcılı, "Analysis of Manipulation of the Russian Federation in the 2016 Presidential Elections of the United States of America within the Scope of Intelligence Techniques", *Güvenlik Bilimleri Dergisi* 8/1 (2019), 140.

[35] Theresa Hitchens and Nilsu Goren, "International Cybersecurity Information Sharing Agreements", *Center for International & Security Studies*, University of Maryland (2017), 14.

technologies. These high levels of control policies carried out by Russia's citizens do not comply with the policies pursued by the western world in the field of cyber security. This has led Russia's developments in cyber security to make as much control as possible with the outside world. This is reflected in the data in the table shared above. Although Russia's distance in the field of cyber security is known to the world public opinion, Russia's cooperation with other countries in this field has been extremely limited. In a study comparing the number of agreements in 47 countries, Russia ranked seventh from the last.[36]

Regarding the countries that Russia cooperated in cyber security field, member states of China and Shanghai Cooperation Organization came to the fore. These agreements made by Russia, which also made agreements with the USA, international organizations, have been realized in a very limited number. Bilateral cooperation between China and Russia, which follow an active policy in the field of cyber security like Russia, has a different meaning compared to other bilateral relations. China has conveyed its experience to Russia on the systems with high control level that Russia wants to realize on its citizens. Russia wanted to enable the activation of a system similar to the system called the *Great Firewall* developed by China by isolating the Internet from the outside world. With this system, although Russian officials stated that they were made to ensure the security of the internet, it also improved Russia's ability to control the access of its citizens to information. Human rights organizations have expressed their concerns about the issue.[37]

Russia has also continued to cooperate closely with states where authoritarian tendencies are observed, in the field of cyber security. This situation will continue to strengthen in the future and it will be indispensable for the stability of the regimes in Russia, China and the countries with authoritarian tendencies. The whole world has witnessed the events in which social media can mobilize the masses in a moment. In societies where opposing thoughts and freedoms are restricted, the prevention of a case that can occur through social media has been inevitable for these countries. For this reason, in the following years, the restriction of

---

[36] Theresa Hitchens and Nilsu Goren, "International Cybersecurity Information Sharing Agreements", 9.

[37] Emily Shervin, "Rusya küresel internet ağıyla bağlantısını kesmeye hazırlanıyor", *DW*, Access: 29.05.2020,
https://www.dw.com/tr/rusya-k%C3%BCresel-internet-a%C4%9F%C4%B1yla-ba%C4%9Flant%C4%B1s%C4%B1n%C4%B1-kesmeye-haz%C4%B1rlan%C4%B1yor/a-47511083, February 14, 2019.

information resources will continue to provide control over communities. Improvements will continue to ensure information security in line with the principles and values of countries not only in the mentioned countries but all over the world.

In addition to protecting its internal security, Russia has tested the use of cyber security technologies for its interests in the field of foreign policy through the operations described in the previous section. Although Russia has firmly dismissed the allegations, the Russian intervention in the 2016 US Presidential election is still intense debate today. With these and many other operations, Russia created cyber attacks as a weapon by creating confusion in the internal politics of the target countries. Cyber security technology, which provides great advantages in both domestic and foreign policy, will emerge as an indispensable tool for states in the coming years as it is today.

One of the problem areas that can be considered as new in foreign policy is internet governance. In this context, large state coalitions, traditional multi-stakeholder internet governance models and policies that focus on expanding the state's role in internet security have been discussed recently. Especially with the Arab Spring, the economic and social effects of the internet have rapidly increased the agendas of policy makers. The war on internet governance, as between authoritarian, non-democratic states. It emerges among states where security is not fully felt because of its liberal, libertarian and cosmopolitan nature. In this context, Russia was evaluated within the second category. Russia is relatively young among these states, with nation-state structure, is evaluated within the states where pluralism, the free market economy and a strong sense of insecurity prevail.[38] In order to eliminate this perception, the concept of "direct democracy via the internet" has been adopted. For this purpose, increasing the digital power, making the state functions more democratic through the internet, are tried to be carried out gradually.[39]

In this context, one of the issues that has been on the agenda in recent years is the "internet fragmentation". The continuation of the leadership race on the internet by governments as well as commercial organizations have increased concerns about this issue. In addition to not providing data security, the development of opportunities to access many data

[38] Julien Nocetti, "Contest and conquest: Russia and global internet governance", *International Affairs* 91/1 (2015), 129.

[39] Julien Nocetti, "Dijital Kremlin: Power and the Internet in Russia", *Russia/NIS Center* (Paris: Ifri): 23.

internationally has increased these concerns. At this point, governments have attempted to develop methods to protect data at their borders.[40]

Since November 1, 2019, Russia has made some regulations on internet law as a new sovereignty area. The main purpose of the arrangements is to protect Russia against attacks from foreign countries via the Internet. In this context, three main targets have been determined. First, an effective and sufficient technical infrastructure regarding internet security will be established within the border. Secondly, Russia aims to create a central control mechanism on the internet, where it can turn digital borders on and off. Third, Russia aims to establish an international internet model and to cooperate closely with the states trying to excel in this field.[41]

Conclusion

Russia quickly saw its shortcomings after the negative experiences it had and developed policies to strengthen itself in the field of cyber security. This effort was a turning point for Russia, especially in 2000, when Putin strengthened the field of cyber security as a state policy and claimed this area from the top screen. Russia has increased its investments in the field of cyber security, reconsidered its institutional structuring and has not been limited to certain state institutions, and has ensured the solid construction of Russian cyber capacity. These reforms were not limited only to state institutions.

Russia made serious efforts in 2000s in order to increase its cyber attack capacity. As a result of its strategy, Russia, which has become one of the most important cyber powers in the international system, wanted to use this power as a means of pressure and sanction in solving foreign policy problems.

Russia has taken steps to strengthen cyber domination in the private sector, based on state security. It has used this cyber power in foreign policy to be compatible with its interests. With the hybrid war method, gains in favor of Russians were achieved in Georgia and Ukraine. In addition to using cyber security technologies in neighboring countries and regional interests, Russia has conducted cyber operations to rival states. In this context, Russia's cyber attacks targeting the information systems of Estonia

[40] William J. Drake, Vinton G. Cerf and Wolfgang Kleinwächter, "Internet Fragmentation: An Overview", *World Economic Forum*, (January 2016), 7-8.

[41] Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law' Tightening Control and Accelerating the Splinternet", *German Council on Foreign Relations (DGAP Analysis*) 2 (January 2020), 2-3.

in 2007 are an example of this. Also, cyber activities of Russia during the Georgian War in 2008, which supports the effects of a conventional war with information technologies, draw attention. In addition, the cyber attacks against Lithuania in 2008 and Kyrgyzstan in 2009, and the "new generation" war concept introduced during the Ukraine intervention in 2014, can be evaluated as examples of how Russia used its capacity in cyber space as a method of pressure and coercion with its neighbors.

The debate on intervention in the US Presidential elections, which has been expressed frequently in the world public opinion since 2016, continues today. The claims that the Russians intervened in the US elections led the country to a process that could lead to the dismissal of US President Donald Trump. Besides the damage has occurred in the belief of transparency of US citizens to their states. It also posed a security concern for US allies. Cyber security, which has emerged as a new war zone, has emerged as an area that should be invested in countries in the coming years as it is today. In addition, countries with authoritarian tendencies such as Russia and China have seen cyber security as a means to keep their citizens under tighter control, unlike Westerners. This situation has created a new area of conflict between the West and Russia.

Instead of trying to ensure the personal security of the Western world in the cyber space, Russia followed the stricter way of control developed by China. The two countries signed bilateral agreements with each other in the field of cyber security. However, although the western world sees cyber security as a tool for personal security, their sincerity in this matter is discussed. Because of the scandalous developments that emerged, the secret behavior of the USA, such as Russia and China, that could neglect freedom has emerged. In this case, the information war shows itself in every field. Some of the activities that Russia and China have explicitly carried out can be carried out by the USA if desired.

Developments in cybersecurity continue quite far from transparency. This gray area, where even the most basic rights of people can be easily suspended, has paved the way for bigger negativities in the future. As a result, competition in cybersecurity should continue in cooperation and understanding, unlike the arms race before World War I. Otherwise, the days that can cause a great crisis for the world do not seem far away.

References

Acar, Hasan. "Küresel Terörün Uluslararası Politikadaki Yeni Aktörü: Hibrit Savaş Modeli". *Küresel Terör ve Güvenlik Politikaları*. ed. Hasan Acar. Ankara: Nobel Akademik Yayıncılık, 2020, 57-71.

Balta, Pınar Hilal. "İsrailli istihbaratçılar BAE'li şirket için Tel Aviv'deki işinden ayrılıyor". *Timeturk*, October 17, 2019. Access: 28.05.2020. https://www.timeturk.com/israilli-istihbaratcilar-bae-li-sirket-icin-tel-aviv-deki-islerinden-ayriliyor/haber-1251495.

BBC News, "Trump Rusya'nın ABD seçimlerine müdahale ettiğini kabul etti". July 17, 2018. Access: 28.05.2020. https://www.bbc.com/turkce/haberler-dunya-44866605.

Connell, Michael and Sarah Vogler. "Russia's Approach to Cyber Warfare". *CNA Analysis & Solutions* (2017).

Cyber Security Intelligence. "What is the GRU & Who Does It Hack?". Uploaded on November 22, 2018. Access: 28.05.2020. https://www.cybersecurityintelligence.com/blog/what-is-the-gru-and-who-does-it-hack-3904.html.

Darıcılı, Ali Burak. "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi". *U.U. International Journal of Social Inquiry* 7/2 (2014): 1-16.

Darıcılı, Ali Burak. "Analysis of Manipulation of the Russian Federation in the 2016 Presidential Elections of the United States of America within the Scope of Intelligence Techniques". *Güvenlik Bilimleri Dergisi* 8/1 (2019): 133-150.

Darıcılı, Ali Burak and Barış Özdal. "Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi". *Ahmet Yesevi Üniversitesi Türk Dünyası Sosyal Bilimler Dergisi (BİLİG)*. Avrasya'nın Siyasal İktisadı Özel Sayısı (2017): 121-146.

Drake, William J., Vinton G. Cerf and Wolfgang Kleinwächter. "Internet Fragmentation: An Overview". *World Economic Forum*. January (2016): 1-80.

Epifanova, Alena "Deciphering Russia's 'Sovereign Internet Law' Tightening Control and Accelerating the Splinternet", *German Council on Foreign Relations (DGAP Analysis*). No. 2, January 2020, 1-11.

Federal Service of Security of the Russian Federation. "Structure: Tasks and Powers of the Federal Security Service of Russia". http://fso.gov.ru/struct/zadachi_polnomochiya/, Accsess: 07.06.2020.

Globalsecurity. Intelligence. "Federal Protective Service (FSO) Federal'naya Sluzhba Okhrani". Access: 28.05.2020.

https://www.globalsecurity.org/intell/world/russia/fso.htm.

Hitchens, Theresa and Nilsu Goren. "International Cybersecurity Information Sharing Agreements". University of Maryland*: Center for International & Security Studies* (2017).

Iasiello, Emilio "Russia and China Are Making their Information Security Case". *The Cyber Research Data Bank*. Access: 28.05.2020. https://www.cyberdb.co/russia-and-china-are-making-their-information-security-case/.

ITU. "Cyberwellness Profile Russian Federation". *Global Cybersecurity Index & Cyberwellness Profiles*, (2015): 389-391. Access: 28.05.2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol: O'Reilly Media, 2012. Access: 29.05.2020.

Kaspersky. "DDoS saldırısı nedir?". https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks.

McKinsey Global Institute. "The Age of Analytics: Competıng in a Data-Driven World". Executive Summary, December 2016. Access: 28.05.2020. https://www.alvaroriascos.com/mineriadatos/The-age-of-analytics-Executive-summary.pdf.

Nocetti, Julien. "Dijital Kremlin: Power and the Internet in Russia". *Russia/NIS Center*. Paris: Ifri, 2011.

Nocetti, Julien. "Contest and conquest: Russia and global internet governance". *International Affairs* 91/1 (2015): 111–130.

Öztürk, Senem. "Jeopolitiğin Rusya Federasyonu'na Etkilerinin Kuzey Kafkasya-Gürcistan Güney Osetya Çerçevesinde İncelenmesi". *Güvenlik Stratejileri* 9/17 (2013): 201-242.

Pasha Sharikov. "Understanding the Russian Approach to Information Security". *European Leadership Network*, January 16, 2018. Access: 28.05.2020. https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/.

Pernik, Piret. "The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine". *Hacks, Leaks and Disruptions Russian Cyber Strategies*. Eds. Nicu Popescu and Stanislav Secrieru. Paris: European Union Institute for Security Studies, 2018.

Pringle, Robert W. "Federal Security Service: Russian Government Agency". *Britannica*. Access: 28.05.2020. https://www.britannica.com/topic/Federal-Security-Service.

Refsdal, Atle, Bjornar Solhaug and Ketil Stolen. *Cyber-Risk Management*. SpringerBriefs in Computer Science. Switzerland: Springer International Publishing, 2015.

Roskomnadzor. "Statute of Roskomnadzor". Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (The Federal Service for Supervision of Communications, Information Technology, and Mass Media). Access: 28.05.2020. http://eng.rkn.gov.ru/about/.

Russia National Security and Defence Policy Handbook: Vol 1 Strategic Information and Basic Laws. Washington: International Business Publications, 2007.

Shervin, Emily. "Rusya küresel internet ağıyla bağlantısını kesmeye hazırlanıyor". *DW*. February 14, 2019. Access: 29.05.2020. https://www.dw.com/tr/rusya-k%C3%BCresel-internet-a%C4%9F%C4%B1yla-ba%C4%9Flant%C4%B1s%C4%B1n%C4%B1-kesmeye-haz%C4%B1rlan%C4%B1yor/a-47511083.

Soldatov, Andrei and Irina Borogan. "Russia's approach to cyber: the best defence is a good offence". *Hacks, Leaks and Disruptions Russian Cyber Strategies*. Eds. Nicu Popescu and Stanislav Secrieru. Paris: European Union Institute for Security Studies, 2018.

Sunçkale, Cevher. *Çeçen Savaşı*. Ankara: Sam Yayınları, 1995.

The Ministry of Foreign Affairs of the Russian Federation. *Doctrine of Information Security of the Russian Federation*. Approved by Decree of the President of the Russian Federation. No. 646 of December 5, 2016.

Yazgan, Ruşen Eşref. *Muhaberat Muhaberatı Bilgi Harbi Genel Değerlendirmeler ve ABD, Rusya Çin Örnekleri*. 2013.