Protecting the Besieged Cyber Fortress: Russia's Response to Cyber Threats

Martti Kari
University of Jyväskylä, Finland
martti.j.kari@jyu.fi

Abstract: The Information Security Doctrine of the Russian Federation (RF) defines the threat to information security as a complex of actions and factors that represent a danger to Russia in the information space. These threats can be information-psychological (i.e., when the adversary tries to influence a person's mind) or information-technical (i.e., when the object of influence is the information infrastructure). The information infrastructure of the RF is a combination of information systems, websites, and communication networks located in the territory of the RF, or those used as part of international treaties signed by the RF. A cyber threat is an illegal penetration or threat of penetration by an internal or external actor into the information infrastructure of the RF to achieve political, social, or other goals. Cyber threats against Russia are increasing and becoming more diverse. The Russian assessment of the cyber threat contains the same besieged fortress narrative as the country's other threat assessments do. In this narrative, Russia is surrounded by hostile states and non-state actors in cyberspace. The sources of the cyber threat are Western intelligence services, terrorists, extremist movements, and criminals. To protect itself against cyber threats, Russia is increasing its digital sovereignty by preparing to isolate the Russian segment of the Internet, RUNET, from the global Internet. Russia is also improving the protection of its critical information infrastructure. To protect itself against cyber threats but also to monitor the opposition, Russia has increased surveillance of RUNET and banned user anonymity. Russia is also making an effort to replace imported information and communication technology (ICT) with Russian production. This paper discuss Russia's defense against cyber threats. After the introduction, the paper begins with a description of the Russian cyber threat perception. The main section then discusses Russia's response to this threat. This study uses grounded theory, an appropriate method for this subject because little theoretical and structured information has, to date, been published on the Russian response to cyber threats. The study data are drawn from official Russian documents such as strategies, doctrines, laws, and presidential decrees.

Keywords: Russia, cyber threat, cyber defense, cyberspace

1. Introduction

According to Russian authorities, the formation of cyberspace as a domain of warfare poses a threat to the Russian Federation's (RF) national interests (PP-2796, 2014) in the information space. According to the Doctrine of Information Security of the RF, Information *space* is a complex of information, objects of informatization, information systems, networks, and information technology. *Informatization* refers to social, economic, and technical processes for adopting and expanding information technology in society and throughout the country as well as to secure access to information resources. Information space includes subjects creating, generating, and processing information; subjects developing and using information technology; or subjects managing information security. It also includes mechanisms regulating the information relations in society. (UP-646, 2016.)

The threat to information security has two dimensions. First, it can be *information-psychological*, which is aimed at influencing the human mind, including its moral and intellectual world, social policy, psychological orientation, and the ability to make decisions. Second, the threat can be *information-technological*, which influences information technology systems (Kamyshev, 2009). The Russian concept of the information-technological threat corresponds to the Western concept of cyber threat. According to the Russian definition, cyberspace[1] is a limited part of the information space. Cyberspace is an environment formed by a set of communication channels on the Internet and other networks, the technological infrastructure that ensures their functioning, and any form of human activity carried out through their use. A cyber threat to Russia is an illegal penetration or threat of penetration by an internal or external actor into the information infrastructure of the RF to achieve political, social, or other goals. Cyber security is a complex of conditions under which all components of cyberspace are protected from all threats and undesirable impacts (SBRF, 2013b).

The increased interest in cyberspace as a domain of warfare has also heightened the need for theoretical studies to assess the cyber threat perceptions of different states and their responses to these threats. Although much non-academic information has been published about Russian offensive cyber capabilities and operations, only a limited amount of information has been published about the country's cyber threat scenarios and defensive

[1] киберпространство

cyber capabilities. However, there is enough information in official Russian legal documents to collect at least a satisfactory picture of the Russian perception of cyber threats and Russia's response to those threats. To protect itself against cyber threats, Russia is increasing its digital sovereignty by preparing to isolate the Russian segment of the Internet, RUNET, from the global Internet. Russia is also improving the protection of its critical information infrastructure. As a further means of protection against cyber threats but also as a way to monitor the opposition, Russia has increased surveillance of RUNET and banned user anonymity. In addition, Russia is making an effort to replace imported information and communication technology (ICT) with Russian production.

This paper examines Russia's defense against cyber threats. After the introduction, there is a description of the Russian cyber threat perception. The main section then discusses Russia's response to this threat. This study uses grounded theory, an appropriate method for this subject because little theoretical and structured information has, to date, been published on the Russian response to cyber threats. The study data are drawn from official Russian documents such as strategies, doctrines, laws, and presidential decrees.

2. Russian cyber threat assessment

The National Security Strategy of the Russian Federation (UP-683, 2015) describes the world as polycentric, where the use of force in international politics is increasing. The West tries to maintain its position by containing Russia (UP-640, 2016). This confrontation between Russia and the West has extended to the information space as well because Western countries are using ICT against Russia to achieve their geopolitical goals (UP-683, 2015). The Kremlin sees the international arena as a battlefield, where the battle to disrupt Russia's digital sovereignty is waged every day (Sinovets, 2016). Digital sovereignty[2] means Russia's rights independently determine internal and geopolitical interests in the digital space (Yarovaya, 2013). Russian national interests – such as sovereignty, territorial integrity and constitutional order – are threatened through cyberspace by Western states, but also by terrorists and criminals. Western countries' preparations for information warfare and aspirations to change cyberspace into a war zone threaten Russia's strategic interests in the cyber environment (UP-646, 2016).

President Putin (2016) has stated that because of the risks inherent to digitalization, Russia has had to strengthen its defenses against cyber threats targeted, for example, at Russian infrastructure, the country's financial system, and the state's leadership and management. The aim of the United States is "to destroy strategic balance, to change the balance of power in such a way not just to dominate but to dictate their will to anyone" (Putin, 2015). The USA uses its technological superiority to dominate the information space (UP-646, 2016).

According to President Putin, the Soviet Union was a besieged fortress constantly under threat of attack by the West (Aron, 2008). After the annexation of Crimea, Kremlin's besieged fortress narrative has become one of the primary means for Putin's regime to maintain power (Kolesnikov, 2016). The besieged fortress view can also be seen in Russia's cyber threat perception, in which Russia describes itself as a besieged fortress in cyberspace. The number and severity of dangers and threats have increased in cyberspace, and those threats are shifting to the internal sphere of the RF (PP-2796, 2014). Vladislav Surkov, the First Deputy of Russian Presidential Administration from 1999 to 2011 and one of the main ideologists of the Kremlin, highlighted internal threats and stated in 2004 that "the enemy is at the gate, and not only at the gate because in the besieged fortress there is a fifth column…sponsored by foreign states" (Ovtsarenko, 2004).

The Military Doctrine of Russia (PP-2796, 2014) defines military danger as interstate or internal relations characterized by a combination of factors that can, under certain conditions, lead to a military threat. Such a threat can emerge in these relations when there is a real possibility of the emergence of military conflict between the opposing parties or by the high degree of readiness of a state, a coalition of states or separatist or terrorist organizations to use military force or armed violence. According to the Military Doctrine, military dangers and military threats are expanding to the information space as well as to the internal sphere of the RF. In modern conflicts, information warfare is used as a part of warfare and the enemy is impacted throughout their entire area of operation, including the global information space (PP-2796, 2014).

The Information Security Doctrine of Russia (UP-646, 2016) includes the same visions of an aggressive West discussed in the National Security Strategy and Military Doctrine. Some states are using their technological superiority to dominate the information sphere and to achieve military and political goals. An unbalanced division

[2] For more on Russian Digital Sovereignty, see Kukkola, Ristolainen & Nikkarila, 2017

of responsibilities in running the Internet between the states increases this technological superiority. This prevents the safe functioning of RUNET, because actors outside Russia can block Russia's access to the Internet and destabilize the functioning of RUNET (SBRF, 2012).

The targets of cyber threats in Russian threat perception can be divided into four categories: the national interests of the RF, the information resources of the RF, the information infrastructure of the RF, and the Russian Armed Forces. The national interests of the RF are the inviolability of its constitutional order, sovereignty, independence, national and territorial integrity, and consolidating the RF's status as a leading world power (UP-640, 2016).

One of the threats to Russian national interests in cyberspace is a lack of competitive ICT and the inadequate use of information technology in the production and research and development of future technologies. This technological backwardness in ICT has created a dependence on foreign information technology. Such underdevelopment weakens Russia's cyber defenses, facilitates cyber intelligence operations in Russia, and gives Western special services an opportunity to influence Russia's information resources (UP-683, 2015; UP-646, 2016). The use of foreign ICT challenges Russia's information security management.

The Draft of the Information Security Doctrine 2015 stated that Russia is lagging behind the leading foreign states in the development of competitive information technology, including supercomputers (PUP-1, 2015). In 2013, Russia was at least three to five years behind the USA in ICT (Eliseev, 2013) and five-and-a-half years behind the USA in supercomputing technology (Moukin, 2013). This technological inferiority strengthens the Russian perception of its strategic vulnerability in cyberspace.

The exploitation of cyberspace by foreign intelligence services against Russia and the possibility of cyberspace attacks on the Russian information resource and information infrastructure have increased. Attacks against objects of its critical information infrastructure are becoming more complex, more frequent, more coordinated (UP-646, 2016), and these attacks can have a destructive impact on the infrastructure. Terrorists and extremists are among those creating means to have this kind of destructive impact (UP-203, 2017). These threats can result in a loss of control, the destruction of infrastructure, irreversible negative change (or destruction) of the economy of the country or an administrative-territorial unit or a significant, long-term deterioration in the safety of the population living in these territories (SBRF, 2012b).

Foreign special services, terrorist organizations, and extremist movements are also targeting the information infrastructure and information resources of the Russian Armed Forces (PP-2796, 2014). The main targets of possible cyberspace exploitation and attacks include strategic missile warning and defense systems, air and space defense forces, and strategic missile forces. Attackers may try to weaken the defense capability of these strategically important systems and forces (SBRF, 2013b; PP-2796, 2014). During a pre-war period and in the first phase of any hostilities, the mobilization of the Russian Armed Forces and the deployment of wartime troops to operational areas are potential targets of cyberspace attacks. The logistical systems supporting mobilization and strategic deployment would also be targets of cyberspace attacks before the outbreak of a war (SBRF, 2012; PP-2796, 2014).

3. Defense against cyber threats

The main means of Russian response to cyber threats are improved protection of the critical information infrastructure of the Russian Federation (CIIRF), a pivot to digital sovereignty by isolating RUNET from the global Internet, increased surveillance of RUNET, banning user anonymity online and the replacement of ICT imports with Russia's own ICT production.

One of Russia's national interests in the information sphere is to ensure the sustainable and uninterrupted functioning of the CIIRF (UP-646, 2016). The concept of the CIIRF was discussed already in the Russian Information Security Doctrine in 2000, hereinafter ISD 2000 (PP-1895, 2000). ISD 2000 started to debate the protection of the CIIRF, about which the core question has been the roles and responsibilities of different state authorities in information security (IS) management of the CIIRF. After ISD 2000, the protection of the CIIRF took almost two decades to organize because of the power struggle over IS management between the Federation Security Service (FSB), the Federal Service for Technical and Export Control (FSTEC), and the Russian Armed Forces, and because of the clarification of the responsibilities of private companies and other legal entities for protection.

In 2013, President Putin signed a decree on the creation of a state system for detecting, preventing, and eliminating the consequences of computer attacks on the information resources of the Russian Federation, hereinafter the GosSOPKA[3] Decree (UP-31, 2013). The GosSOPKA system is a combined, territorially distributed complex that includes authorities and means for detecting, preventing and eliminating the consequences of computer attacks on the CIIRF as well as for responding to other incidents. The GosSOPKA Decree of 2013 assigned the IS management related to cyberattacks to the FSB, but the question of the comprehensive protection of the CIIRF remained unresolved until the CII Security Law in 2017. After two drafts of a law for the security of the CIIRF, one in 2006 and the other in 2013, President Putin signed the Law on the Security of the Critical Information Infrastructure of the Russian Federation (FZ-187, 2017), hereinafter the CII Security Law, in July 2017. Its purpose is to define the CIIRF along with the organizational and legal basis of the IS management of the CIIRF to ensure its stable functioning when targeted by computer attacks.[4]

The critical information infrastructure of the Russian Federation (CIIRF) includes objects of critical information infrastructure as well as the telecommunication networks used to organize the interaction of these objects. The objects of the CIIRF are information systems, information and telecommunication networks, and automatic control systems operating in the following sectors: defense, healthcare, transport, communications, credit and finance, energy and fuel, nuclear, rocket and aerospace, mining, metallurgical, and chemical. The threats to the CIIRF include unauthorized access, destruction, modification, blocking, copying, provision, and dissemination of information about an object of the CIIRF (FZ-187, 2017).

In December 2017, it was confirmed that the FSB, which was tasked to create the GosSOPKA system in 2013, would also be the authority to operate GosSOPKA (UP-620, 2017). The processes implemented in the GosSOPKA framework are detecting, attributing, and responding to computer attacks; eliminating the consequences of computer attacks on the information resources of the RF; assessing the IS management situation and cyber threats; and the collection and analysis of information about computer attacks and computer incidents (SBRF, 2014; UP-620, 2017).

The FSB established and operates the National Coordination Center for Computer Incidents (NCCCI) and regional and territorial IS operations centers (SOC). The GosSOPKA SOCs will be established in the Russian Federation on the federal district[5] as well as the subject level.[6] The SOCs can be operated by the FSB, or they can be departmental or corporative SOCs. The common tasks of SOCs include collecting and analyzing information about computer attacks and computer incidents, responding to threats, and eliminating the consequences of computer incidents in information resources (UP-31, 2013).

The Federal Service for Technical and Export Control of the Russian Federation (FSTEC) is a federal executive body charged with ensuring the security of the CIIRF, countering technical intelligence, and the technical protection of information as well as a specially authorized body in the field of export control (UP-569, 2017). The identification and categorization of the objects of the CIIRF are the first steps in the process of securing and protecting it. The categorization of these objects is a process during which a subject in the CIIRF evaluates and categorizes the significance of a CII object according to the instructions of the FSTEC. Significant objects are placed into Category I, II or III. The categorization (i.e., the assigning of a category number to each object) is based on the social, political, economic, and environmental significance of the object for ensuring the country's defense, state security, and law and order. Category I is for the CIIRF's most significant objects.

After the categorization, the FSTEC specifies requirements to ensure the security of critical CIIRF objects as well as requirements to establish security systems and ensure the functioning of these objects. The FSTEC also includes requirements to ensure the security of information and telecommunications networks which are assigned to one of the three categories of significance and which, in cooperation with the Ministry of Telecom and Mass

[3] GosSOPKA is an abbreviation of the Russian phrase "state system for detecting, preventing and eliminating the consequences of computer attacks."

[4] A *computer attack* is defined as the targeting of software and/or hardware in CII facilities (i.e., the telecommunication networks used to organize the interaction of such objects), with a view to violating and/or terminating their operation and/or creating a security risk that is handled by such objects information.

[5] A federal district is a grouping of the federal subjects for governing by federal governmental agencies. There are eight federal districts in Russian Federation.

[6] The subjects of the Russian Federation are the main administrative divisions in Russia.

Communications of the Russian Federation, are included in the registry of significant CIIRF objects. For the banking and finance sector, the FSTEC sets requirements in consultation with the Central Bank of the Russian Federation. The subject of the CIIRF is obliged to follow FSTEC instructions and establish security arrangements corresponding to the CIIRF object's category of significance. The FSTEC is authorized to evaluate the security arrangements of the objects included in the registry (FZ-187, 2017).

The Kremlin considers digital sovereignty one of the country's main national interests in cyberspace. To secure digital sovereignty, Russia is developing RUNET, a national system of the Internet (UP-646, 2016), the functioning of which should be stable and safe in peacetime, in the event of a direct threat of aggression, and in wartime (UP-646, 2016). This entails that it would be possible to disconnect RUNET from the global Internet (Eliseev, 2013). The Ministry of Communications' Information Society program aims to have 99% of RUNET traffic transferred inside Russian borders by 2020. Part of this plan is to duplicate 99% of RUNET's critical infrastructure within Russia (Meduza, 2016).

In December 2018, the State Duma started to discuss draft legislation to improve Russia's digital sovereignty and to ensure the sustainable operation of RUNET in the case of cyberattacks and other aggressive actions from abroad. The draft names the United States as Russia's main cyber threat and states that Russia must take measures to secure the long-term and stable functioning of RUNET and to improve the reliability of Russia's Internet resources (PZF 608767-7, 2018).

The idea of the draft is to create a Russian national system for .ru and .rf domains, and develop a Russian IP-routing system in a way that a minimum amount of Russian Internet traffic would cross the Russian border and be transferred through foreign exchange points and servers outside Russian borders. The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) develops requirements and rules for actors that run or maintain the Internet in Russia. These actors are Internet providers, the owners of communication lines that cross Russia's national borders, the owners of technological communication networks, the owners of anonymous system numbers, and the owners of traffic exchange points (PZF 608767-7, 2018). Russian Internet providers are required to install technical equipment to counter threats to the RUNET. With this equipment, Roskomnadzor would block banned online resources in Russia and monitor compliance with the new traffic routing rules and the use of the new national domain name system. New monitoring equipment would be provided to Internet service providers (ISP) free of charge, subsidized by Roskomnadzor and the Digital Society program.

Roskomnadzor will establish a traffic-exchange registry. Service providers and companies would be forbidden from using Internet exchange points that are not on the registry. The exchange points would be banned from connecting to companies that do not comply with regulations and rules on the use of the Internet. Roskomnadzor will establish a federal agency called the Center for Monitoring and Managing Public Communication Networks. The tasks of this center are to control Internet regulations, collecting information from Russian companies about, for example, their network infrastructures, and their IP addresses, operating the internet exchange registry, and adjusting the country's traffic routing. According to the draft, the system's efficiency will be checked and improved through regular exercises, participation in which would be mandatory (PZF 608767-7, 2018).

The Russian Armed Forces have their own military intranet, which is a closed IT network specially protected against external cyberattacks. This intranet is called the Closed Data Transmission Segment (CDTS)[7] and it is not connected to the global Internet. The computers of CDTS are protected against, for example, connections by uncertified USB drives and external hard drives. The system has its own e-mail service, which allows the transfer of sensitive information, including secret and top secret documents (Tass, 2016).

Increased surveillance of RUNET is part of the RF's struggle against internal threats. The FSB has a mandate to monitor RUNET traffic. The tool for FSB Internet surveillance is the System for Operative Investigative Activities (SORM).[8] Since the 1990s, the operational capabilities of SORM systems have been improved from SORM 1 to SORM 3. SORM 1 collected mobile and fixed line telephone calls. SORM 2 began collecting Internet traffic. SORM

7 Закрытый сегмент передачи данны (ЗСДП)

8 Система технических средств для обеспечения функций оперативно-розыскных мероприятий

3 collects all kinds of communication on social networks, Wi-Fi, e-mails, Internet traffic, mobile calls, and voice-over-Internet. SORM 3 was introduced into operative use in 2014 (Soldatov and Borogan, 2015). ISPs are required to provide the FSB with statistics on all Internet traffic that passes through their servers. ISPs are also required to install SORM devices on their servers, routing all transmissions in real time through the FSB's local offices (PP-538, 2005).

Two laws were signed in 2017 to ban user anonymity on RUNET. Owners of virtual private network (VPN) services and Internet anonymizers are prohibited from providing access to websites banned in Russia. Roskomnadzor has authorization to block sites that provide instructions on how to circumvent government blocking (FZ-276, 2017). Companies registered in Russia as "organizers of information dissemination," including online messaging applications, are prohibited from allowing unidentified users. Those companies are required to identify their users by their cell phone numbers, and the government is tasked with elaborating the identification procedure. Mobile applications that fail to comply with requirements to restrict anonymous accounts will be blocked in Russia (FZ-241, 2017).

The information security of Russia is characterized by a lack of competitive information technology. The level of dependence of Russian industry on western ICT is high. One of the ways to correct Russia's technical backwardness in ICT and protect it against cyber threats is to develop the country's own IT sector by improving its research, development, and production of information (UP-646, 2016). To improve the security of its information infrastructure, Russia has to replace imported ICT software and equipment with Russian-made counterparts and lay the foundation for technological independence in ICT production (UP-203, 2017). President Putin (2018) stated that Russia needs to build its own digital platforms, ones that should be compatible with the global information space. The ISD 2000 (PP-189, 2000) had already identified the backwardness of Russian ICT as one of the main threats to the country's information security. Over the past decade, however, Russia has not managed to reduce the lead of Western countries in this area.

4. Conclusion

The Russian assessment of the cyber threat against it contains the same besieged fortress narrative as the country's other threat assessments do. Hostile state and non-state actors are surrounding Russia in cyberspace and cyber threats against the country are increasing and becoming more diverse. To protect itself against these cyber threats, Russia has taken operational, technical, and legal actions. The most important of these are improved protection of the CIIRF, preparations to isolate RUNET from the global Internet, intensified surveillance and the ban of user anonymity on RUNET, and the aspiration to replace imported ICT with Russian-produced ICT.

Russia is also making significant efforts to increase its digital sovereignty. It is possible that Russia will manage to create technical and operational readiness to at least partly isolate RUNET from the global Internet by the end of 2020. Russia is also improving the protection of its critical information infrastructure. The definition of the CIIRF and the division of responsibilities between authorities to protect it were confirmed by legislation in 2017 and the implementation phase has now started. The National Coordination Center for Computer Incidents (NCCCI), along with part of the regional and territorial IS operations centers, are now operational.

For Russia, the most difficult question in responding to cyber threats is that the country is lagging behind the leading foreign countries in the development of competitive information technology, including supercomputers, and this gap strengthens the Russian perception of its strategic vulnerability in cyberspace. For almost twenty years, Russia has tried, without success, to replace imported ICT software with Russian-made counterparts, and it seems that they will not succeed in the near future either. Russia is attempting to compensate for this lack mainly by isolating RUNET and by protecting the CIIRF.

References

Eliseev I (2013) I shot digital cannon. Rossiyskaya Gazeta No 6085 (109) May 23. (in Russian) https://rg.ru/2013/05/23/ashmanov.html

FZ-187 (2017). Federation Law of the RF 187 on the Security of Critical Information Infrastructure of the Russian Federation. (in Russian), https://rg.ru/2017/07/31/bezopasnost-dok.html

FZ-241 (2017) Federal Law of the RF 241 "On Amendments to Articles 101 and 154 of the Federal Law" On Information, Information Technologies and Information Protection" (in Russian) https://rg.ru/2017/08/04/informacia-dok.html

Meduza (2016) Russia's Communications Ministry plans to isolate the RuNet by 2020. May 13, 2016. Available at: https://meduza.io/en/news/2016/05/13/communications-ministry-plans-to-isolate-runet-by-2020

PZF 608767-7 (2018) Draft of Law On Amendments to Certain Legislative Acts of the Russian Federation. (in Russian) http://www.lexfeed.ru/law/608767-7

Kamyshev, E. (2009). *Информационная безопасность и защита информации.* Information Security and Protection of Information, (in Russia), http://window.edu.ru/resource/033/75033/files/InfoBesop.pdf

Kolesnikov A (2016) Do Russians Want War?. Carnegie Moscow Center. Available at: http://carnegieendowment.org/files/Article_Kolesnikov_2016_Eng-2.pdf

Kukkola, J; Ristolainen, M & Nikkarila, J-P (2017). GAME CHANGER Structural transformation of cyberspace https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398/PVTUTKL+julkaisuja+10.pdf.pdf

Moukin, G. (2013). Supercomputing Gap Seen as Threat to Economy. The Moscow Times. November 28, 2013. https://themoscowtimes.com/articles/supercomputing-gap-seen-as-threat-to-economy-29999

Ovtsarenko Y (2004) Deputy Head of the Presidential Administration Vladislav Surkov: Putin is strengthening the state, not himself. (in Russian) https://www.kompravda.eu/daily/23370/32473/

PP-1895. (2000). Information Security Doctrine of the Russian Federation. http://base.garant.ru/182535/

PP-2796. (2014) Military doctrine of the Russian Federation, (in Russian), https://rg.ru/2014/12/30/doktrina-dok.html

PUP-1. (2015). Information Security Doctrine of the Russian Federation (draft). http://www.worldinwar.eu/information-security-doctrine-of-the-russian-federation-draft/

Putin, V. (2015) Meetingof the Valdai International Discussion Club. : http://en.kremlin.ru/events/president/news/50548

Putin, V. (2016) President's Speech to the Federal Assembly, (in Russian) http://kremlin.ru/events/president/news/53379

PP-538 (2005) [Decree of the Government of the Russian Federation of August 27, 2005 N 538 (ed. Of September 25, 2018) "On Approval of the Rules for Interaction of Communication Operators with Authorized State Bodies Conducting Operational-Investigation Activities. (in Russian) http://www.consultant.ru/document/cons_doc_LAW_55326/

Putin V (2018) President's Speech to the Federal Assembly]. (in Russian) http://kremlin.ru/events/president/news/56957

SBRF. (2012) The main directions of the state policy in the field of ensuring the security of automated systems for managing production and technological processes of critical infrastructure facilities of the RF, (in Russian), http://www.scrf.gov.ru/security/information/document113/

SBRF. (2013) The concept of cybersecurity strategy of the Russian Federation (Draft), (in Russian), http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

Sinovets P (2016) From Stalin to Putin: Russian Strategic Culture in the XXI Century, Its Continuity, and Change. Odessa. Mechnikov National University. http://www.davidpublisher.org/Public/uploads/Contribute/57eb1fe5a12bc.pdf

Soldatov A, Borogan I (2015) The Red Web. New York: Public Affairs

Tass (2016) In the Russian Federation developed the military Internet for the safe exchange of secret information https://tass.ru/armiya-i-opk/3715422

UP-31 (2013) Decree of the President of the Russian Federation of January 15, 2013 N 31c Moscow "On the establishment of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation" (in Russian) https://rg.ru/2013/01/18/komp-ataki-site-dok.html

UP-203. (2017) The Strategy for the Development of the Information Society in the Russian Federation for 2017-2030, (in Russian), http://www.kremlin.ru/acts/bank/41919

UP-640. (2016) Foreign Policy Concept of the Russian Federation (in Russian) http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU

UP-646. (2016) Doctrine of Information Security of the Russian Federation, (in Russian), https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

UP-683. (2015) The National Security Strategy of the Russian Federation, (in Russian), http://pravo.gov.ru/proxy/ips/?docbody=&nd=102385609

Yarovaya M (2013) Igor Ashmanov: "Today information domination is the same as air superiority]. May 1, 2013. (in Russian) https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe

an Honours Degree in Management from Henley University and a Master's and PhD in Informatics from the University of Johannesburg - specialising in strategies for cyber counterintelligence maturity and the security of cyberspace. He has published various academic papers on cyber strategies and cyber counterintelligence maturity. His professional certifications include CISSP, CISM and CCISO.

Dr. Connie Justice has over 30 years' experience in cybersecurity, computer, and systems engineering. She designed courses in cybersecurity curriculum to NSA/DHS Center of Academic Excellence and NIST National Initiative for Cybersecurity Education standards. Research areas include: fake news, industrial controls risk, experiential learning, information and security risk management, digital forensics.

Fredrick Kanobe was PhD candidate at Tshwane University of Technology, South Africa. His research domain is ICT4D.

Mrs. Eleni Kapsokoli is PhD Candidate in University of Piraeus, Department of International and European Studies, Greece. She also holds a bachelor degree from the National and Kapodistrian University of Athens at the faculty of Political Science and Public Administration. She earned her Master's Degree on International Relations and Strategic Studies at the Panteion University of Social and Political Sciences. Her main research interests include international security, terrorism, cybersecurity and cyberterrorism. She is also a researcher in the Institute of International Relations (I.I.R). She is also a PhD Fellow at the European Security and Defence College (ESDC).

Martti J Kari is university teacher and PhD student of cyber security in Jyväskylä University, Finland. He retired as colonel from Finnish Defense Intelligence in the end of year 2017. His last post was Assistant Chief of Defense Intelligence. He has MA in Russian language (1993) and literature and MA in cyber security (2017) in Jyväskylä University. Kari has worked as a university teacher from the beginning of year 2018 In Jyväskylä University. He is specialized in Russian cyber and hybrid warfare.

Kaur Kullman is researching at the US ARL whether stereoscopically perceivable 3D data visualizations would be helpful for cybersecurity analysts, incident responders and other operational roles. He's been in IT since '90s, focusing on cybersecurity since late '00s. His interests are hands-on technical (OS-hardening, malware analysis, pentests), while his duties at EISA were more various.

Kautsarina is a government researcher at Ministry of Communication and Information Technology (MCIT), Republics of Indonesia since 2009. She also works as an ISO 27001 Lead Auditor for public institution since 2011. She is involved in developing policy research and ICT master plan. Now she is full-time PhD student at Computer Science Faculty, University of Indonesia. Her interest is about information security awareness improvement for end-user.

Anthony Keane, MSc, PhD has a background in astrophysics research and computer science and is currently the Head of the School of Informatics & Engineering in the Technological University Dublin, Ireland. He is also a Principal Investigator in the Cyber Security Education & Research Centre with interests in Cyber Bullying, Cyber Warfare and Cloud Forensics.

Thorsten Kodalle is lecture on security policy at the Command and Staff College of the German Armed Forces with a special focus on NATO, Critical Infrastructure and Cyber. He has a diploma in Social Science, assignments as a youth information officer, in the MoD, lecture on management and leadership and supported for several years computer assisted exercises at the Command and Staff College with constructive simulation. He is a member of the NATO research task group "Gamification of Cyber Defense/Resilience", an experienced facilitator of manual wargaming on the operational level for courses of action analysis, for operational analysis, operations research, serious gaming and especially for matrix wargaming.

Tuija Kuusisto is a Senior Ministerial Advisor at Ministry of Finance and an Adjunct Professor at National Defence University and University of Jyväskylä in Finland. Her expertise covers information analysis and management for decision-making, as well as information and cyber security strategies and policies. She have contributed to several international research and experiment projects and working groups organized by EU, UN and OECD. She has about 70 scientific publications in international and national journals, conference proceedings and books.