DIGITAL ACCESS TO SCHOLARSHIP AT HARVARD
DASH.HARVARD.EDU

HARVARD LIBRARY
Office for Scholarly Communication

Words and Actions: Understanding Russia's Information Security Strategy

Citation
Drazdovich, Uladzislau. 2023. Words and Actions: Understanding Russia's Information Security Strategy. Master's thesis, Harvard University Division of Continuing Education.

Permanent link
https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374936

Terms of Use
This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA

Share Your Story

The Harvard community has made this article openly available.
Please share how this access benefits you. Submit a story .

Accessibility

Words and Actions: Understanding Russia's Information Security Strategy

Uladzislau Drazdovich

A Thesis in the Field of International Relations

for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

May 2023

Copyright 2023 Uladzislau Drazdovich

Abstract

Do Russia's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain? The answer to this question is important because Russia increasingly relies on information warfare tactics for trying to gain a geopolitical advantage vis-à-vis America and its allies, as demonstrated by its meddling in the U.S. presidential elections and numerous cyberattacks on critical U.S. infrastructure. Not only scholars but also policy practitioners can benefit from a clear answer to this question. I will aspire to give that answer in this thesis. I will begin my efforts to answer the aforementioned question by providing background and context for my research. Chapter I will also then offer a review of the literature on information security before describing the theoretical framework, methodology, and research design I will rely upon in my study. In Chapter II, I will analyze Russia's main doctrinal documents released between 2011 and 2021 to infer a broad outline of Russia's stated information security strategy. I will then advance a number of propositions regarding Russia's expected behavior and resource allocation decisions in that domain. I will test these propositions in Chapter III by conducting an empirical analysis of Russia's observable behavior in the 2011-2021 research period based on a collection of open-source data. I will contrast and compare Russia's words and actions in Chapter IV, before determining whether Russia's resource allocations and observable behavior in the sphere of information security were indeed consistent with its

stated information security strategy in the research period. Finally, I will offer concluding remarks and outline potential directions for future research in Chapter V.

Frontispiece

Figure 1. Photo of Russian President Vladimir Putin.

Description of Figure 1. Photo: President of the Russian Federation Vladimir Putin holds a meeting with Government members via videoconference. Kremlin.ru, Presidential Executive Office of Russia, July 8, 2022. The photo is licensed under the Creative Commons Attribution 4.0 International license: https://commons.wikimedia.org/wiki/File:Vladimir_Putin_meeting_with_government_ministers_(2022-07-08)_01.jpg

Acknowledgments

I would like to express my sincere gratitude to my research advisor Dr. Michael Miner for providing the inspiration behind this thesis through his fascinating course on Intelligence and International Security.

I am also profoundly grateful to my thesis director Dr. Simon Saradzhyan for his invaluable guidance and feedback throughout the writing process.

My deepest thanks go to my better half Elena, who provided me with unwavering support and encouragement throughout the research and writing of this thesis. Your love and patience were my driving force, and I could not have accomplished this without you.

I also extend my gratitude to my friends and family for their support and encouragement throughout this journey.

Table of Contents

List of Tables

List of Figures

Chapter I.

Introduction

This chapter will open with a brief description of the evolution of Russia’s behavior in the information security (InfoSec) domain from the seventeenth century to the present day. I will then conduct a review of relevant literature on Russia's cyberspace and information security strategies before describing the theoretical framework, methodology, and research design, which I will employ in my thesis. The chapter will conclude with an overview of research limitations and key definitions of my thesis followed by a summary of this chapter’s key points.

A. Background and Context

1. Historical Genesis of Russia’s Approach to Information Security

Russia has a long history of using information warfare (IW) means to accomplish its strategic objectives, both domestically and internationally.[1] Some of the earliest examples of Russian IW date back to the seventeenth century.[2] At the time, Moscow took active measures to stop the dissemination of handwritten letters, spread by foreign states, in which Russian people were called to commit treason and engage in disobedience to their government. Outside the country, IW was waged by Russian intelligence agents

---

[1] Lesley Kucharski. “Russian Multi-Domain Strategy against NATO: information confrontation and U.S. forward-deployed nuclear weapons in Europe.” Lawrence Livermore National Lab. (LLNL), Livermore, CA (United States). 2019. Accessed December 24, 2022. https://www.osti.gov/biblio/1635758

[2] L. V. Vorontsova and D. B. Frolov. *Istoriya i Sovremennost’ Informatsionnovo Protivoborstva* [*History and Modernity of Information Confrontation*], Goryachaya liniya-Telekom, 2006. ISBN 5-93517-283-6.

typically operating out of the country's diplomatic missions on several fronts and under the direct supervision of Russian Emperor Peter I who ruled Russia from 1682-1725. For example, in the Balkans in the early 1700s, Russian diplomats carried out secret information-psychological operations trying to rile the local Orthodox peoples up against Ottoman rule. In Great Britain, whose government opposed Russia's war with the Ottoman Empire, Russian diplomatic intelligence carried out secret propaganda campaigns, spread rumors, and used the local press to discredit public figures who expressed anti-Russian sentiments.[3]

During the Napoleonic Wars of the nineteenth century, the Russian military used information-psychological tactics, including disseminating leaflets to the enemy and local populations, to weaken enemy morale and influence their decision-making. These efforts proved particularly effective as Napoleon's troops experienced increasing challenges as they marched deeper into Russian territory.[4] During World War I, the Russian military employed similar propaganda tactics to incite non-German and non-Austrian ethnic groups to revolt and promote intervention from neutral countries. Although these efforts had little impact on enemy actions, the General Staff gained valuable experience in strategic propaganda during the war years, which it also deployed against the United States.[5]

During the Soviet period, information-technical and information-psychological activities were conducted by the state security apparatus: mainly by Committee for State

---

[3] Vorontsova, *History and Modernity of Information Confrontation…*
[4] Michelle Grise et al. "Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation," RAND Corporation. 2022. ISBN: 978-1-9774-0717-7. Accessed August 29, 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA198-8/RAND_RRA198-8.pdf
[5] Grise, et al. "Rivalry in the Information Sphere…"

Security (the KGB), which was the Soviet Union's main security and intelligence agency, and by the Main Intelligence Directorate of the Soviet General Staff (the GRU), the country's military intelligence agency. By the late 1970s, the Kremlin established an institutionalized system for conducting both covert and overt military and non-military IW operations[6] That system was applied in a variety of ways, including disinformation campaigns aimed at meddling in foreign elections. For instance, during the 1970 general elections in Pakistan, the KGB leaked fabricated documents implicating senior leaders in Pakistani parties in political murders and opposing the creation of Pakistan before 1948.[7] While there is no conclusive evidence tying this disinformation campaign to the election results, the KGB was able to achieve the outcome it pursued.

Another vivid example of the Soviet information-psychological operations occurred ahead of the 1984 presidential election in the United States (U.S.). In that case, the KGB attempted to damage President Reagan's campaign by spreading negative messaging about the candidate, including Reagan's militarism, his role in exacerbating the arms race, his support for repressive regimes, his administration's record of thwarting national liberation movements, as well as Reagan's responsibility for America's tensions with NATO allies.[8] Although the KGB's efforts failed to prevent Reagan's reelection, it discovered that spreading conspiracy theories to sow distrust among certain segments of the American population regarding their government was a more effective way to undermine its adversary than overt interference campaigns.

---

[6] Kucharski, "Russian Multi-Domain Strategy…"

[7] Arjun Kapur and Simon Saradzhyan. "For Russia and America, Election Interference Is Nothing New: 25 Stories." Belfer Center for Science and International Affairs, Harvard Kennedy School. March 22, 2017. Accessed March 7, 2023. https://www.russiamatters.org/analysis/russia-and-america-election-interference-nothing-new-25-stories

[8] Kapur and Saradzhyan, "For Russia and America…"

With the disintegration of the USSR in 1991, and the advent of the digital age in the late 1990s, Russia had to adapt its Soviet-era tactics to take advantage of modern technological capabilities and the digital information ecosystem. However, its general approach towards IW, as well as its interpretation of information security remained largely unchanged. Just as it did during the Cold War, post-Soviet Russia continues to leverage the information environment to influence the military, policymakers, non-governmental organizations (NGOs), and the general public both domestically and abroad. Assuming the same tactics are being employed by the West, the Russian government remains highly distrustful of all foreign content and opinions entering its own information environment. As such, the Kremlin has repeatedly blamed the occurrence of political protests or unrest on information warfare campaigns waged by the U.S. against Russia.[9]

2. Diverging Perspectives between Russia and the West

The Kremlin's approach to information security has been shaped, to a significant extent, by the long history of information confrontation (rus. Informatsionnoe protivoborstvo) between the Soviet Union and the West.[10] This approach, however, differs vastly from that of the West. For one, the Russian and Western conceptualizations of cyberspace and cybersecurity have several fundamental differences. In fact, Russia does not even use the terms "cyberspace" and "cybersecurity" in the majority of its official doctrines. Although a draft of the 2014 *Cyber Security Strategy Concept*, which

[9] "Putin obvinyaet SSHA v provocirovanii protestov [Putin accuses USA in provoking protests]." *The BBC*. December 8, 2011. Accessed July 28, 2022. https://www.bbc.com/russian/russia/2011/12/111208_putin_opposition_protests
[10] Kucharski, "Russian Multi-Domain Strategy…"

was yet to be adopted as of this writing, but which remains available on the website of the Federation Council (the upper chamber of the Russian parliament), contains references to both of these terms.[11] This terminology, however, may be why the draft concept still has not become an official document after more than nine years since its announcement. The use of the well-defined technical terms of "cyberspace" and "cybersecurity" in an official Russian doctrine could potentially undermine Moscow's historical insistence in international forums on the much wider and less defined concepts of "information security."

In their efforts to assure *cybersecurity*, the U.S. and its European allies have traditionally focused on the technical aspects of protecting networks, devices, and data from unauthorized access. In contrast to this approach, Russia's pursuit of *information security* involves – in addition to the software and hardware components – protecting all media used to transmit and share information.[12] As a result, the *ways* and *means* the Kremlin employs to achieve its information security *ends* are not limited to cyberspace and can include a variety of other domains and spheres of society, such as diplomacy, economy, culture, education, mass media, and so on.

When it comes to conducting offensive information operations, Moscow distinguishes between two types of activities: information-technical and information-psychological.[13] Information-technical activities aim to affect the technical systems of the opponent that receive, process, or transmit information. On the other hand, information-

---

[11] "Koncepciya strategii kiberbezopastnosti Rossiyskoy Federacii [The Russian Federation Cybersecurity Strategy Concept]." The Federal Council, Russian Federation. January 10, 2014. Accessed January 29, 2023. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
[12] Keir Giles. "Handbook Of Russian Information Warfare." NATO Defense College. November 2016. ISBN: 9788896898161. Accessed July 28, 2022. https://www.researchgate.net/publication/313423985_Handbook_of_Russian_Information_Warfare
[13] Giles, "Handbook..."

psychological operations are directed not at the technology, but at the minds of the adversary's military personnel and civilian population.[14] Thus, Russia's information warfare operations include not only reconnaissance and efforts to compromise opponents' information and communications technology (ICT), but also activities aimed at demoralizing and weakening these opponents' very societies. Such activities can take the form of news propaganda, disinformation campaigns, public speeches, defamatory video content, and other forms of exerting a desired psychological influence.[15]

The aforementioned major differences in both terminology and conceptualization of information security used by Russia and the West continue to cause confusion and normative disagreement in the international arena. While Western cybersecurity and internet governance experts typically seek consensus on ways to protect a nation's digital networks, Russian diplomats push for increased government oversight of media content.[16] As the world moves further into the information age, these diverging perspectives have significantly exacerbated the ongoing information confrontation between Russia and the West.

3. Information Space as Russia's Strategic Priority

Starting in the late 2000s, Russia began to take steps towards approaching the information space as a strategically important domain. A series of domestic developments, as well as political turmoil in the international arena, have prompted the

[14] Giles, "Handbook..."
[15] Giles, "Handbook..."
[16] Pavel Sharikov. "Understanding the Russian Approach to Information Security," European Leadership Network, January 16, 2018. Accessed July 28, 2022. https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/

Kremlin to create a plan for increasing Russia's IW capabilities. For one, Russia's war with Georgia in 2008 exposed serious deficiencies in the area of information operations. While Russia won the military campaign, enhancing its control over Georgia's separatist regions of South Ossetia and Abkhazia, the common perception among multiple Russian and Western military analysts and the media was that Moscow had lost the information warfare against Tbilisi.[17]

From the start of the conflict, Georgian President Mikheil Saakashvili was able to establish direct communications channels with the world's leading news media. A fluent English speaker, Saakashvili shared his side of the story through op-eds placed in prominent news outlets and provided updates on the situation on the battlefield during live TV interviews.[18] In contrast, Russia's press conferences during the August 2008 war were often led by First Deputy Chief of the General Staff, Anatoliy Nogovitsyn who only presented in Russian.[19] This disparity in outreach was one of the major reasons why Moscow largely failed to frame the narrative about the conflict beyond its domestic audiences. Realizing these shortcomings, in 2008, the Russian Ministry of Defense appointed a new deputy minister Dmitriy Chushkin, tasking him with supervising the

[17] Keir Giles. "'Information Troops' – a Russian Cyber Command?" 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011 © CCD COE Publications.
[18] Alya Samigullina and Natalya Kuklina. "Eto propaganda v tradicii Sovetskogo Souza [This is propaganda in the tradition of the Soviet Union]." *Gazeta.ru.* August 13, 2008. Accessed July 28, 2022. https://www.gazeta.ru/politics/2008/08/12_a_2809214.shtml?updated
[19] Keir Giles. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power." Chatham House. The Royal Institute of International Affairs. March 2016. Accessed July 28, 2022. https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power

development of information technologies and communications of the military department.[20]

The Arab Spring of the 2010s, the Revolution of Dignity in Ukraine in 2014, as well as the 2010 and 2020 revolutions in Kyrgyzstan, also served as major catalysts for Russia's renewed focus on information warfare. The Kremlin saw the fall of established regimes in Ukraine and across the Middle East and North Africa as a direct result of a coordinated information campaign by the U.S. and its allies.[21] This perception was further strengthened by the fact that Western social media platforms, such as Twitter, played a major role in both the Tunisian and Egyptian revolutions by helping galvanize both domestic and international audiences.[22] President of the Russian Academy of Military Sciences Army General Makhmut Gareyev made this assessment in early 2011:

> "Internet networks were implanted in Egypt, Tunisia, and Libya over a two-year period. It started with systematic training for communication checks, without direct calls for unlawful actions. At the right moment, a centralized order was issued across all networks for people to take to the streets."[23]

By that time, the Russian authorities had already begun to emphasize the information space as a prominent element across its main doctrinal documents. For instance, Russia's

---

[20] "Naznachen novyi zamministra oborony [New deputy defense minister appointed]." *Gazeta.ru*. November 24, 2008. Accessed July 28, 2022. https://www.gazeta.ru/news/lenta/2008/11/24/n_1300007.shtml

[21] It is worth noting, however, that this interpretation did not stop then-President Medvedev from joining forces with Barack Obama to set up the U.S.-Russia Bilateral Presidential Commission (BPC) that included a Working Group on Threats to and in the Use of ICTs in the Context of International Security. For more information, see The White House, Office of the Press Secretary. "Joint Statement on the Inaugural Meeting of the U.S.-Russia Bilateral Presidential Commission Working Group on Threats to and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security." Press release. National Archives and Records Administration. November 22, 2013. Accessed March 5, 2023. https://obamawhitehouse.archives.gov/the-press-office/2013/11/22/joint-statement-inaugural-meeting-us-russia-bilateral-presidential-commi

[22] Catherine O'Donnell. "New study quantifies use of social media in Arab Spring." University of Washington. September 12, 2011. Accessed July 28, 2022. https://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/

[23] Giles, "Handbook…"

2010 *Military Doctrine* acknowledged the use of integrated non-military means as a characteristic feature of modern military conflicts.[24] Russia's next military doctrine, which was adopted in 2014, expanded this concept recognizing the use of "political, economic, informational or other non-military measures" among the characteristic features of modern military conflicts.[25] The 2011 *Russian Federation Armed Forces' Information Space Activities Concept* also elevated the information space to the level of the traditional military domains of land, sea, air, and space.[26]

Meanwhile, the political situation within Russia began to show signs of instability. During the 2011 elections to State Duma (the lower and more powerful chamber of the Federal Assembly, the Russian parliament), massive anti-government protests erupted in Moscow and St. Petersburg, which some English-language news media dubbed as the Snow Revolution.[27] Alarmed by the examples of the Arab Spring and color revolutions in the former Soviet republics of Georgia, Ukraine, and Kyrgyzstan, the Kremlin began to take further steps to strengthen its information security by developing both defensive and offensive IW capabilities.

4. Evolution of Russia's Strategic Thinking about Information Security since 2011

Since 2011, information security has become a much more prominent item on the Kremlin's political agenda. On February 26, 2012, a week before the Russian presidential

---

[24] *The Military Doctrine of the Russian Federation*. The Russian Federation. February 5, 2010. Accessed January 2, 2023. https://carnegieendowment.org/files/2010russia_military_doctrine.pdf

[25] *The Military Doctrine of the Russian Federation.* The Russian Federation. No.Pr.-2976, December 25, 2014. Article II, Section 15, Clause a).

[26] *Russian Federation Armed Forces' Information Space Activities Concept*. Ministry of Defense of the Russian Federation. 2011. Accessed February 5, 2022. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

[27] Andrew Osborn. "Bloggers who are changing the face of Russia as the Snow Revolution takes hold." *The Telegraph.* December 10, 2011. Accessed July 28, 2022. https://bit.ly/417SSWa

election, then Prime Minister Putin published an article titled "Security in the world can only be ensured together with Russia," in which significant attention was paid to matters of InfoSec.[28] Expressing his concern about the growing influence of ICT, Putin stated the following:

> "The 'Arab Spring' has also vividly demonstrated that the world's public opinion is currently being shaped by the most active use of advanced information and communication technologies. We can say that the Internet, social networks, mobile phones, etc. have become – along with television – an effective tool for both domestic and international politics. This is a new factor that requires reflection, in particular, so that while continuing to promote the unique freedom of communication on the Internet, we can reduce the risk of its use by terrorists and criminals.
>
> "The concept of "soft power" has also come into greater use - a set of tools and methods for achieving foreign policy goals without the use of weapons, but through information and other levers of influence. Unfortunately, these methods are often used to nurture and provoke extremism, separatism, nationalism, manipulate public consciousness, and directly interfere in the internal politics of sovereign states."

Putin further suggested that non-governmental organizations (NGOs) and other structures were funded and used by foreign interests to destabilize political situations in various states. In conclusion of his more than 6,100-word piece, Putin underscored: "In the information field, we are often outplayed. This is a separate multifaceted issue that needs to be taken seriously." Putin went on to win the March 4 elections, returning to the Kremlin. A year later, he and U.S. President Barrack Obama signed a joint statement on cybersecurity issues.[29] The statement "On a new area of confidence-building

---

[28] Vladimir Putin. "Vladimir Putin: Bezopasnost' v mire mozhno obespechit' tol'ko vmeste s Rossiey [Vladimir Putin: Security in the world can only be ensured together with Russia]. *Rossiyskaya Gazeta* [*The Russian Gazette*]. February 26, 2012. Federal Issue №45(5718). Accessed January 2, 2023. https://rg.ru/2012/02/27/putin-politika.html

[29] Sovmestnoe zayavlenie prezidentov Rossiyskoy Federacii I Soedinennyh Shtatov Ameriki o novoy oblasti sotrudnichestva v ukreplenii doveriya [Joint Statement by the Presidents of the Russian Federation and the United States of America on a New Area of Confidence-Building Cooperation]. Kremlin.ru. June 17, 2013. Accessed January 2, 2023. http://kremlin.ru/supplement/1479

cooperation" recognized the threats stemming from the use of ICT, as well as ICT itself, among the most serious national and international security issues of the twenty-first century.

The evolution of Russia's strategic thinking about InfoSec and IW was also reflected in statements by some of Russia's military strategists who increasingly began to discuss non-military means as alternatives to kinetic force. For instance, in their 2013 article "The Nature and Content of the New Generation of War," Colonel Sergei Chekinov and General Sergei Bogdanov argued that "with the continuous revolution in information technology, to a large extent, victory will be determined by information and psychological warfare."[30] However, such emphasis on IW did not immediately receive unanimous support among Russia's senior military commanders, some of whom voiced their concerns about overreliance on non-contact warfare. For example, in his 2014 column in the Russian newspaper the *Military-Industrial Courier*, General and Doctor of Military Sciences Anatoly Zaitsev wrote:

> "Network-centric and non-contact military activities occupy a prominent space in the modern [military] theory. We should note at once: only those with a very rich imagination can claim that war can be contactless. Its goal is always occupation followed by annexation or coercion of the enemy to peace on favorable terms for the winner. The opposing sides can use however many new types of weapons, military and special equipment, but all of it is designed for firearm damage, destruction of infrastructure, the annihilation of the material and human resources of the enemy."[31]

---

[30] Sergei G. Chekinov and Sergei A. Bogdanov. "Priroda I soderzhanie voiny novogo pokoleniya [The nature and content of the new generation of war]." *Voennaya Mysl'* [*The Military Thought*]. 4 (2013): 12-23.

[31] Anatoly Zaitsev. "Partizanskimi Metodami: Sovremennaya armiya doljna umet' voevat' bez linii fronta [Partisan Methods: Modern army must be able to fight without the frontline]." *Voenno-Promyshlennyi Kur'er* [*The Military-Industrial Courier*]. September 1, 2014. Published in print in issue No.32 (550), September 3, 2014. Accessed July 30, 2022. https://vpk-news.ru/articles/21649

Similarly, General Sergei Surovikin – who would eventually become the commander of the Russian Aerospace Forces – cautioned at a 2014 military academy conference that "absolute conviction that modern wars will be exclusively contactless, brief, and conducted only in air and space can lead to irreversible consequences in the future."[32]

Still, there was growing recognition among Russia's military and political scientists that the country could not compete with the U.S. in conventional warfare, either economically, militarily, or technologically. As such, the interest in finding new asymmetric response paths continued to grow. With the development of the digital age, information weapons came to be recognized as an effective and affordable solution.

On November 9, 2012, less than a year after the release of the *Conceptual Views on the Activity of the Armed Forces in the Information Space*, Vladimir Putin appointed Army General Valery Gerasimov as the Chief of the General Staff of the Russian Armed Forces, and First Deputy Defense Minister, replacing General Nikolay Makarov.[33] In February 2013, Gerasimov published an article in the *Military-Industrial Courier* titled "The Value of Science is in the Foresight."[34] The article contained excerpts from his recent speech on hybrid warfare at the Russian Academy of Military Sciences. In that speech, Gerasimov presented a new theory of modern warfare that relies on information-technical and information-psychological tactics not as auxiliary means, but as the main way to achieve victory over an opponent:

---

[32] Sergey V. Surovikin. "Forms for Employing and Organizing Command and Control of a Joint Troop (Force) Grouping in the Theater of Military Activity," *Vestnik Akademii Voennykh Nauk* [*Bulletin of the Academy of Military Sciences*], Vol. 1, No.46, 2014.
[33] "Genshtab vozglavil Valeriy Gerasimov [Valery Gerasimov takes the helm of the General Staff]." Interfax. November 9, 2012. Accessed July 30, 2022. https://www.interfax.ru/russia/275082
[34] Valery Gerasimov. "Cennost' nauki v predvidenii [The Value of Science is in the Foresight]." *Voenno-Promyshlennyi Kur'er* [*The Military-Industrial Courier*]. February 26, 2013. Accessed July 30, 2022. https://vpk-news.ru/articles/14632

> "And the 'rules of war' themselves have changed significantly. The role of non-military methods in achieving political and strategic goals has increased, which in a number of cases have significantly surpassed the power of weapons in their effectiveness.
>
> "The emphasis in the methods of confrontation is shifting towards the widespread use of political, economic, informational, humanitarian and other non-military measures implemented with the use of the protest potential of the population. All this is complemented by covert military measures, including the implementation of information confrontation measures and the actions of special operations forces. The open use of force, often under the guise of peacekeeping and crisis management, is only adopted at some stage, mainly to achieve final success in the conflict."[35]

Further, Gerasimov underscored the importance of defending Russia's interests outside its territory by combining information, military, technological, diplomatic, economic, and cultural tactics. To help usher in Russia's superiority in this new generation of warfare, Gerasimov called for closer collaboration between the Armed Forces and military science. After being republished in the English-language magazine *Military Review*, the article became widely known as the "Gerasimov Doctrine."[36] I should note here that the application of the term "doctrine" to Gerasimov's article is somewhat of a misnomer, which has been contested by many Western experts, including British researcher Mark Galeotti who claims to have coined the term.[37] Still, Russian arms control and nuclear weapons specialist Dr. Igor Sutyagin noted that key elements of the Gerasimov Doctrine have since been integrated into the draft of the Russian *Military Doctrine* of 2014.[38]

---

[35] Gerasimov, "The Value of Science…"

[36] Valery Gerasimov. "The Value of Science Is in the Foresight." *Military Review*. 2016: January–February. pp. 23-29. Accessed July 30, 2022. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/

[37] Mark Galeotti. "I'm Sorry for Creating the 'Gerasimov Doctrine.'" *Foreign Policy*. March 5, 2018. Accessed January 2, 2023. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

[38] Igor Sutyagin. "Russian Forces in Ukraine." Royal United Services Institute. Briefing Paper. March 2015. Accessed February 13, 2023. https://rusi.org/explore-our-research/publications/briefing-papers/russian-forces-ukraine

Russia also demonstrated its use of the methods outlined by Gerasimov during its annexation of Crimea in 2014. There, Russia was able to accomplish its ends by deploying less than 10,000 troops against the 16,000 Ukrainian military personnel stationed in Crimea.[39] Russia's active use of information-technical and information-psychological capabilities helped it to successfully attain its aim of seizing and annexing Crimea. During the first stage of the annexation, Russia targeted Ukrainian computer systems with a combination of sophisticated malware known as Snake, Uroburos, and Turla.[40] Russian troops then raided Crimean communication centers and tampered with fiber-optic cables, cutting mobile, landline, and internet connections between the peninsula and mainland Ukraine. Additionally, Ukrainian government websites, news outlets, and social media were also disabled by Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.[41] The second stage involved the use of information-psychological tactics, including intimidation, bribery, and heavy propaganda transmitted through the internet and Russian news media.[42] By successfully orchestrating this combination of conventional military and information warfare strategies, Moscow was able to thwart local resistance in Crimea, avoid the use of firepower, and win in the court of public opinion among the Russian population.

In more recent years, Russia's increasing information warfare operations have brought the issues of InfoSec to the forefront of international relations. In the U.S. alone,

---

[39] Janis Berzinš. "Russia's New Generation Warfare In Ukraine: Implications For Latvian Defense Policy." National Defence Academy of Latvia. Center for Security and Strategic Research. Policy Paper #02. April 2014.
[40] Jen Weedon. "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine." FireEye. 2015. In Kenneth Geers (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn: NATO CCD COE Publications. ISBN 978-9949-9544-5-2.
[41] Weedon, "Beyond 'Cyber War'…"
[42] Berzinš, "Russia's New Generation Warfare…"

the utilities, information technology (IT), healthcare, food, and agriculture sectors, and even, arguably, the minds of the American public have been impacted by Russian cyber and IW operations, through the use of malware and ransomware attacks, cyber espionage, and mass disinformation campaigns.

A wave of cyberattacks, including the 2018 NotPetya ransomware attack that targeted Ukraine, but caused damage across the globe; the 2020 hack of the SolarWinds software company in the U.S.; and a series of international ransomware attacks of July 4, 2021, have cost national economies of the U.S. and multiple other countries billions of dollars. U.S. cybersecurity experts, such as former head of the Cybersecurity and Infrastructure Security Agency Chris Krebs, believe Russian military and intelligence agencies were behind both the NotPetya and SolarWinds attacks while Russia-based ransomware gang REvil claimed responsibility for the July 4, 2021, hacking campaign.[43]

The need to address the rising wave of high-profile cyberattacks, along with Russia's repeated attempts to influence the outcome of both the 2016 and 2020 U.S. presidential elections, were two of the major reasons why President Joe Biden agreed to meet his Russian counterpart Vladimir Putin on June 16, 2021.[44] During the meeting,

---

[43] For more information about these cyberattacks, see: Ellen Nakashima. "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes." *Washington Post*. January 12, 2018. Accessed January 29, 2022. https://wapo.st/3IBY7Gk; Isabella Jibilian and Katie Canales. "The US is readying sanctions against Russia over the SolarWinds cyberattack. Here's a simple explanation of how the massive hack happened and why it's such a big deal." *Business Insider*. April 15, 2021. Accessed January 29, 2022. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12; Charlie Osborne. "Updated Kaseya ransomware attack FAQ: What we know now." *ZDNET*. July 23, 2021. Accessed January 29, 2022. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

[44] For more information on the Geneva summit, see: Vladimir Soldatkin and Steve Holland. "Far apart at first summit, Biden and Putin agree to steps on cybersecurity, arms control." Reuters. June 16, 2021. Accessed February 1, 2022. https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/; For more information on Russia's attempted influence on the U.S. elections, see: Intelligence Community Assessment 2020-00078D. "Foreign Threats to the 2020 US Federal Elections," National Intelligence Council. March 10, 2021.

which took place at Villa La Grange in Geneva, Switzerland, President Biden emphasized the need to establish "some basic rules of the road" on issues of information security that both nations could follow.[45] Subject-matter experts on both sides, however, remain skeptical about a near-term possibility of formal bilateral agreements between Russia and the U.S. This skepticism is rooted in several factors, including the two sides' long-time mutual mistrust and stark differences in both terminology and approaches to cyberspace and information security. It is also rooted in the poor state of U.S.-Russian relations, which reached a freezing point due to multiple factors, including Russia's aggression in Ukraine.[46]

Given the rapid development of information technologies across all sectors of the global economy, as well as increasing tensions between Moscow and the West, issues pertaining to Russia's InfoSec strategy will likely remain high on the U.S. and its allies' foreign policy agendas in the foreseeable future. As such, this study aims to answer the following research question: *do Russia's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain?* To do so, I will analyze Russia's stated InfoSec strategy in the 2011-2021 period, identify its key elements, priorities, and areas of focus, and assess how well they correspond with Russia's real-world actions. Answering this question will allow us to better understand whether Russia's stated InfoSec strategy can serve as a reliable predictor of its future behavior.

[45] Soldatkin and Holland, "Far apart at first summit…"
[46] Laudern Zabierek, et al. "US-Russian Contention in Cyberspace Are 'Rules of the Road' Necessary or Possible?" Belfer Center for Science and International Affairs, Harvard Kennedy School. June 2021. Accessed August 18, 2022. https://www.russiamatters.org/analysis/us-russian-contention-cyberspace-are-rules-road-necessary-or-possible

As Moscow demonstrates an increasing reliance on information warfare as a means of achieving its political ends, it is important that the U.S. and the West develop a better understanding of Russia's InfoSec strategy. By determining whether Russia's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain, I hope to establish a better understanding of Moscow's actual strategic interests and behavior in the information domain. I also hope that my answer to that question will help illuminate the actual *ends, ways,* and *means* of Russia's information security strategy. This knowledge can help the U.S. and its Western allies to better anticipate and defend themselves against malignant behavior that Russia is likely to continue to exhibit towards them in this domain in the near future. They will be able to make more informed decisions regarding their own long-term *ends, ways*, and *means* in the field of InfoSec. Moreover, this knowledge can also help Western policymakers to pursue a more productive dialogue amongst themselves, as well as with their counterparts from non-Western countries, including Russia, on the topic of information security.

B. Literature Review

The information domain has always been an arena for strategic competition between Moscow and Washington, though relations improved during the post-Cold War era that began shortly after Mikhail Gorbachev's ascent to power in 1985 and continued until the end of Dmitry Medvedev's sole presidential term and the beginning of Putin's third presidential term in 2011-2012. Long before the advent of digital technologies and the World Wide Web, the strategies and tactics of IW employed by Soviet Russia became the subject of academic research.[47] As multiple scholars have pointed out, today, the Russian government continues to consider the information space as a key domain for interstate competition, recognizing that it can be effectively used to influence populations, both domestically and abroad. As the world became increasingly interconnected, the Kremlin has been able to successfully apply many of its time-tested Soviet IW techniques by simply updating them for the digital age.

While reviewing literature for this thesis, I mostly, but not exclusively, focused on the following kinds of works: articles in peer-reviewed journals and books by credentialed subject-matter experts that (1) examine Russia's strategic behavior in the information sphere; (2) advance theories pertaining to interstate confrontation in the information sphere; (3) analyze and compare Russia's information operations and information security strategies and tactics to those of other states. Included below is a succinct overview of some of the most influential literature on the subject, as well as some of the lesser-known but more specialized studies of Russia's cyberspace and information security strategies.

Some of the earlier Western assessments of the Russian InfoSec strategy were undertaken by Lieutenant Colonel Timothy L. Thomas, an analyst at the U.S. Army's Foreign Military Studies Office, Fort Leavenworth, Kansas. In his 1998 article "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," Thomas compares and identifies key differences between the

---

[47] For more information on pre-World Wide Web research on the Soviet Union's information warfare tactics, see Glenn Curtis and Jim Nichol. *Annotated Bibliography on Psychological Operations*, Federal Research Division Library of Congress, April 1989. Accessed February 2022. https://apps.dtic.mil/sti/pdfs/ADA302447.pdf

Russian and the U.S. approaches to information operations.[48] One of the primary differences highlighted by Thomas is Russia's focus on "information-psychological" operations that aim to shield its society from foreign manipulation through various information campaigns, which can, in turn, generate political instability. Indeed, the author identifies what is perhaps the most distinctive quality of Russia's strategic InfoSec thinking. To this day, Russia's concern about and its focus on shielding its population from the information-psychological influence of the West remains a stark throughline across its strategic doctrines.

Thomas identifies three primary factors that prompted Russia to develop its own unique approach to IW. First, unlike the U.S., at the time of his 1998 study, post-Soviet Russia was going through a difficult transition period characterized by institutional and philosophical instability, which made its population susceptible to psychological manipulation by promises of economic and social prosperity. The second factor is the different genesis of the Russian traditional military thinking, which was determined by a unique set of geographic, economic, and ideological considerations. Finally, economic, technological, and infrastructure limitations have forced Russia to focus on information-psychological applications of IW while the U.S. prioritized areas of technology.

The paper's main, if inevitable, shortcoming is that it is more than twenty years old, and some of the factors identified by the author have undergone a significant evolution, thereby changing Russia's approach to IW. For example, while Russia's IT resources were extremely scarce in the 1990s, the country significantly modernized its IT

[48] Timothy L. Thomas. "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations." *Journal of Slavic Military Studies*, 1998, Vol.11, No.1, pp. 40-62. Accessed August 14, 2022. https://community.apan.org/cfs-file/__key/docpreview-s/00-00-08-56-53/1998_2D00_03_2D00_01-Dialectical-Versus-Empirical-Thinking-_2800_Thomas_2900_.pdf

infrastructure during the second decade of the twenty-first century. Despite its age, however, Thomas' insightful assessment illuminates many aspects of the Kremlin's approach to information security.

When it comes to more recent literature on the subject, Professor at Georgetown University's School of Foreign Service Ben Buchanan can certainly be considered as one of the most influential authors on InfoSec issues over the past decade. In his 2017 book *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations,* Buchanan highlights the propensity of the cyber domain to generate acts of war.[49] He explains that the difficulty of signaling intent and capabilities in cyberspace contributes to the security dilemma. Popularized by Robert Jervis in the 1970s, the security dilemma explains how actions taken by one state to increase its security cause other states to fear for their own security, which leads to tensions and an arms race that ultimately decrease the security of the original state.[50]

Buchanan argues that the offense-defense balance in cyberspace does, in fact, favor offensive operations. Despite the resources needed to research, develop, and carry out a cyberattack, identifying, preventing, and remediating cyber intrusions has proven to be more difficult for states to maintain successfully. Additionally, states are, in fact, incentivized to conduct proactive cyber operations against other states to both strengthen their defensive capabilities, as well as build a competitive technological advantage. As a result, states will inevitably interpret any network intrusions as threatening to their security, which, in turn, is likely to escalate conflict potential.

---

[49] Ben Buchanan. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford University Press; 1st edition (February 1, 2017). ISBN-10: 0190665017.
[50] Robert Jervis. "Cooperation Under the Security Dilemma." *World Politics* 30, no. 2 (1978): 167–214. Accessed October 15, 2022. https://doi.org/10.2307/2009958

The author admits, however, that his framework is somewhat hindered by the issue of attribution. For the cybersecurity dilemma to be relevant, states need to know whose activity threatens their security, which is often difficult given the highly covert nature of cyber operations. Nevertheless, Buchanan's application of the traditional security dilemma paradigm offers an original perspective for analyzing state behavior in cyberspace that continues to be highly relevant today.

Russian scholar Oleg Shakirov (2020) brings yet another traditional IR concept into the cyber domain – deterrence. To understand how Russia and the U.S. apply the concept of deterrence in cyberspace, the author conducts a comparative analysis of several doctrinal documents issued by the two countries.[51] He then compares how the statements pertaining to cyber deterrence made by both countries are reflected in their policies. Shakirov notes that Russia first mentions cyber deterrence in its 2011 *Armed Forces' Information Space Activities Concept*, the 2014 *Military Doctrine*, as well as the 2016 *Information Security Doctrine*. He concludes that, in terms of presenting its efforts, Russia focuses primarily on defensive measures, exercising a "deterrence by denial" approach.

According to Shakirov, in the U.S., the concept of cyber deterrence has a longer history and is better detailed in the country's doctrines. The *International Strategy to Secure Cyberspace* adopted in 2011 during the administration of President Barack Obama, as well as the U.S. 2017 *National Security Strategy* and the 2018 *National Cyber Strategy* adopted during President Donald Trump, all list cyber deterrence as one of the

[51] Oleg I. Shakirov. "Kto pridet s kibermechem: podhody Rossii I SsHA k sderzhivaniyu v kiberprostranstve [Whoever Comes with a Cyber Sword: Russian and U.S. Approaches to Deterrence in Cyberspace]." *Journal of International Analytics*. 2020;11(4):147-170. Accessed Aug 15, 2022. https://www.interanalytics.org/jour/article/view/326

priority areas for protecting the American people and their way of life. However, while Russia underscores the role of diplomacy and international agreements to deter cyber threats, the U.S. outlines a broader set of tools, adopting a "deterrence by punishment" approach, according to Shakirov.

Although he offers an interesting point of view on the U.S. and Russia's approaches to cyber deterrence, Shakirov's research could benefit from a more robust demonstration of empirical actions taken by both states that would support his conclusions. For example, the author claims that Russia exercises a deterrence-by-denial approach when it comes to cyberattacks. However, he relies mostly on official statements by the Russian government that, indeed, tend to be defensively oriented. But one's words do not always match one's actions, and a stated approach does not equal an exercised one. While Shakirov acknowledges that Moscow is often accused of conducting offensive cyber operations, he immediately dismisses these allegations based solely on the Russian government's official denials of its involvement. Given the breadth of existing literature examining Russia-attributed cyberattacks in the U.S., Estonia, Georgia, and Ukraine, these activities should have been factored into the author's conclusions.

Another piece of literature worth highlighting in this review is Ben Buchanan's highly acclaimed 2020 book in which he advances a theory about interstate confrontation in the information sphere.[52] The author of *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* posits that cyber operations have become important tools for "geopolitical shaping." Using several detailed case studies to support his claims, Buchanan argues that cyberattacks aren't as effective for signaling as conventional

---

[52] Ben Buchanan. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Harvard University Press; 1st edition. February 25, 2020. ISBN-10: 0674987551.

weapons. To be effective, signaling requires a highly visible and easily interpretable action with predictable ramifications. Cyberattacks can rarely be that straightforward. Moreover, revealing the identity of the perpetrator can yield valuable information to the opponent, which may enable it to better defend itself against future attacks.

As a result, states instead use cyber operations to shape geopolitical environments. Be it Russia's meddling in the U.S. presidential elections or the U.S. and Israel using the Stuxnet virus to sabotage Iran's nuclear program, Buchanan argues that the cyber domain has become an arena where states struggle for geopolitical advantage. Further, the author warns that, as modern technologies and powerful encryption become more widespread, the U.S. and its allies are slowly losing their "homefield advantage" stemming from the global cyberinfrastructure developed by American technology companies.

While the author spends a lot of time delving into the technical aspects of some of the offensive cyber operations detailed in his case studies, in this book, he neglects to discuss the technical elements of cyber defense. The book would have benefited from a discussion of how the featured states' information/cybersecurity strategies informed their offensive operations. Buchanan could also have made a better effort to explain how the strategic logic of using cyberattacks as tools for geopolitical shaping fits within the existing IR scholarship. Nevertheless, Buchanan's book makes a rich academic contribution to modern information warfare literature while serving as an accessible primer on the role of cyber operations in modern geopolitics.

While Buchanan examined the nature of interstate confrontation in the information domain, cybersecurity expert Daniel Moore focused specifically on the military component of cyber operations pursued by Russia and three other countries. In his 2022 book *Offensive Cyber Operations: Understanding Intangible Warfare,* Moore explores how states implement their military offensive network operations (MONOs) into their overall strategies.[53] He focuses his analysis on four of the most prolific actors: the U.S., Russia, China, and Iran. After examining the states' respective MONO strategies, the author highlights both their advantages and shortcomings.

According to Moore, the Russian strategic theory involves a holistic perception of conflict, which often blurs the lines between wartime and peacetime operations. As such, Russia has integrated MONOs into a broader spectrum of its influence, misinformation, and propaganda operations. Moore argues that Russia is generally war-averse and most of its offensive operations in cyberspace do not meet the threshold of warfare. Instead, Russia uses a combination of low-intensity, sporadic activities to subvert and diminish its opponents primarily by eroding civilian will rather than targeting the military. However, the author notes that the Russian approach does not often yield the desired impact due to technical and operational limitations.

Perhaps the most distinctive conceptual contribution of Moore's book lies in the author's classification of offensive operations as "presence-based" and "event-based." According to Moore, presence-based operations are "lengthy intrusions that culminate in an attack," while event-based operations "represent immediate attacks against networks and equipment."[54] Although this dichotomy raises important strategic and operational considerations, Moore could have offered a more thorough examination of the concept.

---

[53] Daniel Moore. *Offensive Cyber Operations: Understanding Intangible Warfare.* Oxford University Press. August 1, 2022. ISBN-10: 0197657559.
[54] Moore, *Offensive Cyber Operations…* p. 5.

Most event-based cyberattacks – especially at the state level – require long periods of presence-based activities to gain necessary access to the target.[55] As such, the distinction between presence-based and event-based offensive operations becomes somewhat muddled. Additionally, it is not clear whether the author distinguishes between electronic warfare operations (EW) and cyberattacks within this established classification. These minor shortcomings, however, do not diminish the overall importance of Moore's effort. Through a wide range of case studies, Moore demonstrates how and why states develop their own information warfare capabilities based on strategic objectives that are often entirely different from one state to another.

Policy researcher Bilyana Lilly and defense analyst Joe Cheravitch (2020) use a historical perspective to offer a useful analysis of Russia's cyber strategy by examining the institutional cultures that have shaped Russian security agencies over time.[56] They find that, although Russia's official doctrine projects a defensive cybersecurity posture, statements made by Russian military elites suggest a growing interest in employing cyber weapons due to their effectiveness and affordability.

To further understand this contradictive nature of Russia's approach to cyberspace, Lilly and Cheravitch examine the organizational culture and historical evolution of Russia's cyber and information operations conducted by the KGB and parts of the national armed forces in the Soviet times, as well as by the Federal Security

---

[55] For example, it took the U.S. and Israel several years to develop and deploy the Stuxnet computer virus against an Iranian uranium enrichment facility. See: Jim Finkle. "Researchers say Stuxnet was deployed against Iran in 2007." Reuters. February 26, 2013. Accessed January 28, 2023. https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226

[56] Bilyana Lilly and Joe Cheravitch. "The Past, Present, and Future of Russia's Cyber Strategy and Forces." 2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.). 2020 © NATO CCDCOE Publications, Tallinn.

Service (FSB), and The Main Directorate of the General Staff of the Armed Forces (GU, a.k.a. GRU) in post-Soviet times.[57] The authors conclude that the development of Russia's strategic cyber operations was facilitated by the shift in the 2010s when the GU replaced the FSB as the primary conductor of offensive cyber operations. Thus, the GU's inherently more risk-tolerant organizational culture informed Russia's more aggressive modern-day approach to information warfare.

Lilly and Cheravitch offer an illuminating and well-structured analysis of how Russia's cyber and information operations evolved over time. Indeed, Russia's aggressive behavior in cyberspace in recent years, from the hacking of the Democratic National Committee in 2016 to the NotPetya ransomware in 2017, has made countless headlines. However, the authors' omission of Russia's foreign intelligence service, the SVR from their analysis stands out as a notable oversight. Responsible for some of the biggest cyberattacks in recent history, the SVR plays a major role in shaping Russia's IW tactics.[58] For example, one could argue that Moscow's more recent activity has demonstrated a focus on long-term and more covert offensive cyber operations. The 2019-2020 SolarWinds breach, which the U.S. government attributed to the SVR, went undetected for at least fourteen months. [59] This is much longer than the average

[57] The Main Directorate of the General Staff of the Armed Forces (GU) is commonly known and still often referred to by its previous name – the Main Intelligence Directorate (GRU). It was renamed as the GU by President Vladimir Putin in 2018. For additional details, see: Aleksey Druzhinin. "Kak menyalos' nazvanie otechestvennoy razvedki [How the name of the national intelligence changed]." *Press Service of the President/*TASS. November 2, 2018. Accessed October 11, 2022. https://tass.ru/info/5752382

[58] Alert (AA21-116A) "Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders" The U.S. Cybersecurity & Infrastructure Security Agency. April 26, 2021. Accessed December 23, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa21-116a

[59] "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government." The White House. April 15, 2021. Accessed December 12, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

cyberattack discovery time of ninety-five days in 2019, according to a report by cybersecurity firm CrowdStrike.[60] Could this shift to more covert operations be explained by the historic differences in the SVR's and the GU's organizational cultures? If so, the already compelling reasoning advanced by Lilly and Cheravitch would prove to be even more difficult to dispute.

The historical genesis of Russia's approach to IW and InfoSec was further explored in another recent study by a team of researchers at RAND's National Defense Research Institute. Titled "Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation," the study examines Russian approaches to information warfare (or, as it is often referred to in the Russian literature, *informatsionnoe protivoborstvo*, or IPb) as a component of the country's strategic thinking.[61] The authors conduct an extensive review of the Russian military-scientific literature and major strategic documents to outline the evolution of Russian IPb operations from the late eighteenth century to the present day. They find that Russia's perception of being in a constant state of information confrontation with the West plays a major role in shaping its foreign policy. Yet, despite being widely discussed in the Russian literature, Moscow's approach to IPb is yet to be formalized in a unified official doctrine, according to the RAND study.

The authors suggest that the Russian military-scientific literature can be a useful resource for the U.S. intelligence community to better understand Russia's intentions and activities in the information domain. They also highlight the need for additional research

---

[60] Saheed Oladimeji and Sean M. Kerner. "SolarWinds hack explained: Everything you need to know." *TechTarget*. June 29, 2022. Accessed December 12, 2022. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
[61] Grise, et al. "Rivalry in the Information Sphere…"

into how Russia applies IPb in hybrid warfare, uses it as a soft power tool, and what it means for the prospects of establishing effective international governance in cyberspace. While the authors do not attempt to discern the difference between words and deeds when it comes to Russia's cyber activities, the report is well-researched and provides an excellent overview of the Russian conceptions of IPb. The authors draw on a variety of sources, including Russian documents, literature, and interviews with Russian experts to provide a comprehensive analysis of the issue.

Delving further into the subject of the Russian IW and InfoSec strategies, British expert on Russian security issues Kier Giles examined how the Russian government sees its role in cyberspace in his 2012 paper "Russia's Public Stance on Cyberspace Issues."[62] To better understand how Moscow's approach to information security impacts its behavior, Giles analyzes two of Russia's most recently released (at that time) public documents pertaining to cyberspace: the *Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space* (2011),[63] and the *Draft Convention on International Information Security* (2011).[64] The author finds that, while the West traditionally insists on the free flow of information in cyberspace, Russia and its allies argue that national sovereignty also extends to the information domain. Thus, states should be able to control content residing in their sovereign information space.

After identifying some of Russia's key InfoSec concerns, Giles tests them by conducting a case study. To do so, he examines Moscow's informational and political

---

[62] Keir Giles. "Russia's Public Stance on Cyberspace Issues." 2012 4th International Conference on Cyber Conflict. C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 © NATO CCD COE Publications, Tallinn.
[63] *Information Space Activities Concept...*
[64] *Russian Draft Convention on International Information Security*. The Ministry of Foreign Affairs of the Russian Federation. September 22, 2011. Accessed July 31, 2022. https://bit.ly/3ZCGhJd

response to the protests that erupted following the disclosure of the State Duma election results in December 2011. He finds that the government's contradictory response to online dissent reflects the mixed views among Russian leaders regarding the extent of internet regulation. Giles predicts that Russia will likely continue to advocate stricter cyberspace regulations. Highlighting a key challenge for Western governments, the author concludes by saying that, despite using similar language, Russia and the West have fundamental differences in their approach to cyberspace.

While Giles attempts to connect Russia's doctrinal statements to its real-world actions, he stops short of presenting a comprehensive outline of Russia's strategic objectives within its overall InfoSec strategy. Giles' decision to conduct a case study based on a particular short-term event (civil protests over election results in December 2011), limits the utility of his study for assessing the practical impacts of Russia's official views regarding InfoSec on its strategic long-term behavior. Furthermore, the Russian government has since adopted new versions of its military, national security, and information security doctrines, as well as its foreign policy concept. All of them contain important statements about Russia's view of InfoSec, thus demanding further assessment.

The different approaches to information security between Russia and the U.S. were further explored by researcher Blagovest Tashev, Lieutenant Colonel Michael Purcell (Ret), and Major Brian McLaughlin (Ret) in their 2019 paper "Russia's Information Warfare Exploring the Cognitive Dimension."[65] The authors note that Russia increasingly relies on IW as a strategic tool for interstate competition, which was demonstrated during its annexation of Crimea in 2014, as well as by its interference in the

[65] Blagovest Tashev, Michael Purcell, and Brian McLaughlin. "Russia's Information Warfare Exploring the Cognitive Dimension." *MCU Journal* vol. 10, No.2. Fall 2019.

2016 U.S. presidential elections. To better understand Russia's approach to competing in the information domain, the authors analyze its national security documents, including the *Russian National Security Strategy* (2015)*, The Foreign Policy Concept of the Russian Federation* (2016)[66], and *The Military Doctrine of the Russian Federation* (2014).[67] They find that all three documents reflect Russia's concern with the increasing use of the information domain for interstate competition.

The authors also note a key difference in the way Moscow and Washington approach IW. While in the U.S. information warfare is primarily concerned with wartime operations by the military, Russia follows a much more holistic interpretation of the term, engaging both military and civilian methods and employing both national and non-governmental institutions to achieve its goals. Moreover, it aims at not only targeting the adversary's computer networks or communications infrastructure, but also the minds of the entire population of the targeted state, affecting people's perceptions, shaping their views, and guiding their decisions. Consequently, the Kremlin sees the U.S. attempts to promote human rights, democracy, and Western international order as a similar form of IW, targeting the established norms and social cohesion of the Russian people.

By focusing on the cognitive dimension as an integral part of the information space, Tashev et al. highlight an important concept that is becoming increasingly explored in the scientific literature on the subject. However, there seems to be no agreement on where exactly cognitive warfare (CW) fits in relation to other offensive and defensive activities, such as information warfare, cyber operations, phycological

[66] *Foreign Policy Concept of the Russian Federation.* Ministry of the Foreign Affairs of the Russian Federation. December 2016. Accessed February 27, 2023. https://www.voltairenet.org/article202038.html
[67] *Military Doctrine…*

operations, and electronic warfare. For instance, James Lewis (2018) argues that cyberattacks can produce powerful cognitive effects that can be even more important than those produced by kinetic weapons.[68] On the other hand, scholars like Zac Rogers (2021)[69] and Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla (2020) insist on distinguishing CW from other forms of operational information warfare.[70] While Tashev et al. do not attempt to settle this debate, they succeed in accurately capturing the divergence in Moscow's and Washington's interpretations of the term "information warfare."

When it comes to Russia's approach to ensuring security within its domestic information sphere, Russian scholar Maksim Kotlyarov offered an insightful assessment in his 2017 article "Controlling the Uncontrollable: the Russian Government's Internet Strategy."[71] While reviewing the Kremlin's cyberspace policy between 2012-2016, Kotlyarov argues that the government's actions were driven by two primary considerations. First, Moscow views the global internet as an instrument of U.S. foreign policy that threatens the Russian government's political sovereignty. Second, the internet and social media enable Russian citizens to mobilize and organize political protests. Kotlyarov points out that the Kremlin considers both of these factors as threats to national

---

[68] James A. Lewis. "Cognitive Effect and State Conflict in Cyberspace." *Center for Strategic and International Studies (CSIS).* September 26, 2018. Accessed December 11, 2022. https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace

[69] Zac Rogers. "The Promise of Strategic Gain in the Digital Information Age: What Happened?" *The Cyber Defense Review* Vol. 6, No. 1 (WINTER 2021), pp. 81-106.

[70] Alonso Bernal et al. "Cognitive Warfare: An Attack on Truth and Thought." NATO and Johns Hopkins University. 2020.

[71] Maksim V. Kotlyarov. "Kontroliruya Nekontroliruemoe: Strategiya Rossiyskogo Gosudarstva v Internete [Controlling the Uncontrollable: the Russian Government's Internet Strategy]." *Vestnik Permskogo Universiteta* [*Perm University Courier*]. *Politology*. 2017. №3. Accessed August 14, 2022. https://cyberleninka.ru/article/n/kontroliruya-nekontroliruemoe-strategiya-rossiyskogo-gosudarstva-v-internete

security. Thus, he explains why the task of controlling cyberspace was assigned primarily to special services rather than civil departments. I find the author's assessment to be accurate as Russia openly states similar concerns in several of its strategic doctrines. For instance, in its 2015 *National Security Strategy*, Russia talks about increasing attempts by some countries to use information and communication technologies to exert their influence and manipulate public awareness.[72]

Kotlyarov argues that the Russian government sees cyberspace as a domain that needs to be controlled the same way as physical territory, leveraging its capabilities for the benefit of the state. However, he cautions that simply controlling local infrastructure is not enough to ensure control of the information space due to the internet's decentralized nature and millions of users involved in producing and sharing information online. While falling short of a formal scientific study, Kotlyarov's article offers a valuable local vantage point on Russia's InfoSec concerns.

Researcher at the Institute for Media and Communication Studies in Berlin, Anna Litvinenko further examined Russia's stance on cyberspace, as well as the main factors that influenced its development, in her 2021 paper "Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty."[73] She finds that the Russian strategic narrative on internet policy has evolved, depending on the balance of perceived threats and opportunities presented by global connectivity. The author notes that, while Western countries have traditionally ensured information security by focusing on

---

[72] *Strategy of National Security of the Russian Federation*. Ministry of Defense of the Russian Federation. December 2015. Article II, Section 21.
[73] Anna Litvinenko. "Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty." *Media and Communication.* (ISSN: 2183–2439) 2021, Volume 9, Issue 4, Pages 5–15. Accessed August 14, 2022. https://doi.org/10.17645/mac.v9i4.4292

protecting infrastructure, Russia focuses on controlling information flows and content itself. According to Litvinenko, the three key elements of Moscow's quest for internet sovereignty are: (1) control over data; (2) control over infrastructure; and (3) promotion of the Russian internet governance initiatives at the international level. Litvinenko's conclusion seems to fall in line with Russia's observable behavior in recent years, which I will examine in greater detail further in this thesis.

The Soviet Union's approaches to information warfare and information security have been studied quite extensively during the Cold War years. However, as evident from this literature review, with the rapid development of digital infrastructure and Russia's increasingly assertive behavior in recent years, Moscow's strategic thinking in the information domain has once again become a topical field for academic research. Still, despite having conducted robust preliminary research, none of the existing scholarship I was able to find attempts to discern, on a systemic level, whether the observable actions of the Russian government are consistent with its stated information security strategy in 2011-2021.

Thomas (1998), Tashev et al. (2019), Lilly and Cheravitch (2020), and Grise et al. (2022) offer robust examinations of the evolution of Russia's approach to IW and InfoSec. Moore (2022) helps us better understand Russia's modus operandi in cyberspace by comparing it to those of other major cyber powers, like the U.S., China, and Iran. Buchanan (2017), and Shakirov (2020) offer original perspectives on assessing state behavior in cyberspace through the prism of classic IR theories, while Kotlyarov (2017), and Litvinenko (2021) provide insightful analyses of how Russia addresses its information security concerns through internet regulation. All of these works add valuable insights into the processes that have shaped Russia's approaches to InfoSec and IW. However, the question raised by this thesis seems to fall beyond the scope of their research. Of the authors reviewed in this section, Giles' attempt (2012) to connect Russia's doctrinal statements to its real-world actions comes closest to achieving the goal, which I pursue in this thesis. Still, his attempt falls short, in my view, because he analyzes only one of Russia's fully adopted doctrinal documents and conducts only one case study focused on a short-term event. These limitations prevent him from identifying the full range of objectives of Russia's InfoSec strategy, which is something that this thesis aspires to accomplish.

Establishing whether Russia's words and actions regarding its InfoSec strategy are in agreement will require both a more comprehensive analysis of its official doctrinal statements and a broader overview of its resource allocation decisions at the state level. This thesis aspires to accomplish both. Building on the literature reviewed above, I will develop and employ a new framework for analyzing the words and actions of Russia's InfoSec strategy. In doing so, I will aspire to answer this thesis' central question of whether Russia's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain. By offering an answer to this question, this thesis will not only expand the body of academic knowledge about Russia's InfoSec strategy but will also introduce a new approach that could, perhaps, be used by future assessments of Russia's strategic behavior in the information domain.

C. Theoretical Framework

As mentioned earlier, this research aims to answer the following question: *do Russia's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain?* My approach to answering this question will be primarily rooted in the strategic theory of international relations. I have chosen this theory because, as I explain below, it provides an effective framework for exploring why and how state actors choose and pursue strategies. Advanced by such renowned scholars, as Colin Gray,[74] Thomas Schelling,[75] MLR Smith,[76] and Harry Yarger,[77] this theory has become an important tool for understanding the strategic behavior of political actors, both state and non-state. It is Yarger's definition of strategy at the nation-state level that this thesis relies upon: "the art and science of developing and using the political, economic, social-psychological, and military powers of the state in accordance with policy guidance to create effects that protect or advance national interests relative to other states, actors, or circumstances."[78]

It follows from strategic theory that actors, both state and non-state, achieve these effects by defining and rationally aligning *ends, ways*, and *means*. In this triad, "*ends*" refers to the end goals of the state actor, "*means*" refers to the resources available to it, while "*ways*" refers to how those resources are allocated to accomplish the end goals.[79] It is the relationships within this triad that strategic theory studies. It assumes that all

---

[74] Colin S. Gray. *Theory of Strategy*. Oxford University Press. 2018. ISBN-10: 0198800673.
[75] Thomas Schelling. *The Strategy of Conflict.* Harvard University Press. 1981. ISBN 9780674840317.
[76] M.L.R. Smith. "Strategic Theory: What it is…and just as importantly, what it isn't." *E-International Relations.* April 28, 2011. ISSN 2053-8626. Accessed August 17, 2022. https://bit.ly/3EHRSi3
[77] Yarger, Harry R. *Strategic Theory for the 21st Century: The Little Book on Big Strategy.* U.S. Army War College Press, 2006. Accessed December 14, 2022. https://press.armywarcollege.edu/monographs/723
[78] Yarger, *Strategic Theory…*
[79] Frank, L. Jones. "Toward a Strategic Theory of Terrorism: Defining Boundaries in the Ongoing Search for Security." *Strategic Studies Institute, US Army War College.* 2012. Accessed August 17, 2022. https://www.jstor.org/stable/pdf/resrep12116.11.pdf

political actors, who constitute this theory's central unit of analysis, have interests and that these actors will make rational decisions in pursuit of those interests. This theory also considers the value system and the wider strategic environment guiding political actors' pursuit of interests. It argues that political actors, both state and non-state, use strategies to create more favorable outcomes by choosing how (in what *ways*) they will use the resources available to them (*means*) to accomplish the goals (*ends*) outlined by their policy.[80] When exploring the political actors' use of strategies, strategic theorists observe moral neutrality and refrain from making moral judgments regarding the *ends, ways*, and *means* the actors choose.[81]

In my view, strategic theory provides a sound methodological basis, logical framework, and essential terminology that can be used to explore why and how state actors, such as the Russian state, choose and pursue strategies in an ever-changing environment. Therefore, it is the aforementioned central tenets of this theory that will guide my examination of how (in what *ways)* a political actor, such as the Russian state, allocates its economic, political, military, social-psychological, and other *means* to achieve its strategic *ends* in the information domain.

D. Methodology and Research Design

Having explained my decision to choose strategic theory as the theoretical foundation of my thesis, I will now explain what methodology and research design I will rely upon when applying this theory to answer the research question. Specifically, I have chosen a qualitative approach to conduct my research. There are two primary reasons

[80] Yarger, *Strategic Theory…*
[81] Smith, "Strategic Theory…"

why I have made this choice. First, my primary sources for outlining Russia's InfoSec strategy include a collection of textual documents. Qualitative analysis is better suited for these types of unstructured non-numerical data. Second, I expect my research process to be emergent by design, which means it cannot be tightly structured from the beginning. For example, I cannot make specific propositions about Russia's expected behavior until I have collected and interpreted the data pertaining to its stated InfoSec strategy. Qualitative methods will enable me to remain flexible in my research process, allowing the discovered data to drive the direction of the study, which would be difficult to do using either quantitative or mixed research methods.

Applications of the qualitative research approach generally begin with making a series of assumptions with a theoretical lens employed to better understand complex phenomena.[82] It involves the collection and inductive analysis of data that establish patterns or themes. These identified themes can then be interpreted allowing the researcher to generate propositions that can be further developed into testable hypotheses.

To outline Russia's stated InfoSec strategy, I will conduct a thematic analysis of the country's main doctrinal documents. Thematic document analysis is a qualitative research method that involves identifying and analyzing recurring themes or patterns in a set of documents.[83] Using this analytical method, I will select, evaluate, and synthesize statements pertaining to information security that are contained in the Russian strategic doctrines.

---

[82] John W. Creswell and Cheryl N. Poth. *Qualitative Inquiry & Research Design: Choosing Among Five Approaches*. Fourth edition. Los Angeles: SAGE, 2018.
[83] Glenn, A. Bowen. "Document Analysis as a Qualitative Research Method." *Qualitative Research Journal,* vol. 9, no. 2, 2009. ISSN: 1443-9883. Accessed August 17, 2022. https://www.emerald.com/insight/content/doi/10.3316/QRJ0902027/full/html

While Russia does not currently have a dedicated national cybersecurity strategy (NCSS), its official views on assuring national information security are articulated in a number of its strategic documents, such as the *National Security Strategy*, *Foreign Policy Concept*, *Information Security Doctrine*, *Military Doctrine*, and *Armed Forces' Information Space Activities Concept*. Therefore, I selected these documents as primary sources for analysis to understand the key elements of Russia's InfoSec strategy.

It is worth noting, however, that Russia may be currently developing a standalone cybersecurity doctrine.[84] On January 10, 2014, the government published a concept of the future doctrine, outlining its purpose, focus, and role within the larger framework of Russia's strategic documents. However, since it is not a functioning doctrine at this time, I chose to omit it from my selection of analyzed documents. Another document omitted from this analysis is the 2015 version of the *Maritime Doctrine of the Russian Federation*.[85] This document lays out how the Russian Navy plans to address the main military and naval issues facing the nation. However, it does not touch on Russia's strategic objectives in the information domain and is therefore not relevant to this particular study. Finally, the current version of Russia's nuclear deterrence doctrine titled *Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence* (2020), was also excluded from my analysis.[86] While the document includes a brief mention of "information policy in the area of nuclear deterrence," it does not expand on what that policy is, nor does it advance any actionable steps pertaining to information security.

---

[84] See "The Russian Federation Cybersecurity Strategy Concept."

[85] *The Maritime Doctrine of the Russian Federation.* The Russian Federation. 2015. Accessed August 30, 2022. https://digital-commons.usnwc.edu/rmsi_research/3

[86] *Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence.* The Russian Ministry of Foreign Affairs. June 2, 2020. Accessed February 27, 2023. https://archive.mid.ru/en/web/guest/foreign_policy/international_safety/disarmament/-/asset_publisher/rp0fiUBmANaH/content/id/4152094

To help uncover common themes pertaining to Russia's InfoSec strategy that are present across the examined documents, I will organize relevant statements according to four categories:

1. Perceived InfoSec threats
2. Opportunities to defend or advance InfoSec interests
3. Proposed domestic policy actions
4. Proposed foreign policy actions

I chose these categories because they represent the fundamental elements of strategic logic, which include:

- Assessing the strategic environment (identifying *perceived InfoSec threats*)
- Defining desired *ends* (*opportunities to defend or advance InfoSec interests*)
- Identifying and/or developing the *means* (resources or capabilities needed to accomplish the goals likely to be mentioned under the *opportunities* and *proposed policy actions* categories)
- Outlining the *ways* to use the available *means* to achieve the defined *ends* (the *proposed domestic and foreign policy actions* categories will help explain how those goals can be accomplished)[87]

Having categorized relevant statements made across the examined documents, I will identify common themes permeating Russia's strategic doctrines. These key themes, in turn, will provide me with a broad outline of the *ends*, *ways*, and *means* of Russia's InfoSec strategy. Equipped with a better understanding of Russia's stated InfoSec

---

[87] Steven Heffington, Adam Oler, and David Tretler. *A National Security Strategy Primer.* National Defense University Press, Washington, D.C. 2019. Accessed December 18, 2022. https://bit.ly/3Ia1nr7

strategy, I will advance a number of testable propositions regarding Russia's expected behavior and resource decisions pertaining to the information domain.

However, words and actions do not always match, and a state's actions can differ from its declared strategy. Therefore, to understand whether Russia's stated InfoSec strategy can serve as a reliable predictor of its future behavior, I will identify Russia's actions in this sphere and then contrast those with its stated goals. To do so, I will test my propositions by conducting an empirical analysis of state behavior based on a collection of qualitative research data in the form of government documents, official publications from national, international, and local organizations, scholarly articles, and media reports, and other primary and secondary sources. If Russia followed the objectives uncovered through my thematic analysis of its doctrines, I would expect to find that the government has implemented domestic and foreign policies that support its declared goals, including the allocation of resources to the corresponding sectors of its economy in the research period. Alternatively, if the Russian government's actions in this sphere did not correspond with its stated objectives in that period, then I would expect to find no significant efforts made by the government in order to pursue them.

To bind the temporal scope of my study, I chose to limit my research period to the eleven years between 2011 and 2021. I selected 2021 because it was the last full calendar year at the time when I began my research for this thesis in 2022. There are three main reasons why I chose 2011 as the beginning of my research period.

First, 2011 was the year when Russia released its first official doctrinal statement on InfoSec, the *Armed Forces' Information Space Activities Concept*. While Russia expressed IT-related concerns in its prior doctrines, such as the 2000 *Information*

Security Doctrine, for instance, these earlier documents did not feature as many specific goals and objectives pertaining to the information domain. My second reason for starting with 2011 is that this was the period when, prompted by a series of anti-government revolutions abroad, as well as growing political dissent at home, Moscow began to significantly elevate its rhetoric around InfoSec, and cyberspace in particular, as areas of strategic focus (I have highlighted parts of this historical genesis of Russia's approach to information security in Section A of this thesis). Finally, these eleven years ushered in numerous revolutionary technological breakthroughs that have qualitatively changed the way people generate, share, and consume information. The widespread adoption of smartphones and 4G networks, as well as the rise of social media platforms and digital news networks instantly connected billions of people around the world, creating unprecedented potential for social influence and political activism. This new and rapidly evolving digital information environment presented the Russian government with a completely new set of threats to mitigate and opportunities to pursue, which makes the 2011-2021 period particularly fascinating for this research.

E. Research Limitations

It should also be noted that an evaluation of whether a state is following its stated strategy has its limitations. Due to the scope of my research, I will need to make a conscious effort to avoid selection bias by using the evidence that supports my propositions and ignoring the evidence that does not. I will mitigate this limitation by using multiple sources and different types of evidence to support my conclusions.

Additionally, a state's strategy is never static and can change based on world events and arising challenges. The doctrinal documents analyzed in this study span the period of 2011-2021. As such, the government's statements made in earlier documents can become outdated as it adapts to the changing strategic environment. To address this limitation, I will analyze the evolution of Russia's strategic narrative regarding InfoSec by comparing all editions of these doctrinal documents within the research period. These include both the 2013 and 2016 editions of the Russian *Foreign Policy Concept*, and the 2016 and 2021 editions of the *Information Security Doctrine*. By assessing the consistency of messaging among all reviewed doctrines, I will be able to conclude whether the *ends, means*, and *ways* of Russia's InfoSec strategy remained consistent throughout the research period.

Another potentially limiting factor in this research is that a state does not always reveal its true aims and strategic goals in public documents. In fact, it may purposefully distort its true objectives and identified threats in order to mislead its geopolitical adversaries. To avoid speculation and conjecture regarding the hidden intentions of Moscow's political leadership, this study focuses only on Russia's *stated* InfoSec strategy and *revealed* policy actions.

I should also note that the Russian government is notoriously secretive about its military and security apparatus. Publicly available versions of Russian InfoSec doctrines do not explicitly discuss specific information operations. The government rarely makes public statements about the organization and operation of its InfoSec departments, and all of its military and security spending is classified. Thus, this research can only evaluate Russia's actions based on unclassified, publicly available information.

Finally, my chosen framework of strategic theory has its own limitations that I ought to acknowledge in this research. One of strategic theory's main criticisms is that it appears to treat collective decisions as if they were made by unitary actors. This thesis may appear to do the same by attempting to assess the actions of the Russian State as a monolithic actor. However, I see this as a necessary simplification to advance and test the proposed research question. Additionally, one can argue that the consolidation of Russia under Putin's increasingly authoritarian – if not semi-totalitarian – regime, indeed makes it a monolithic state actor.

Strategic theory has also drawn criticism for assuming that actors behave rationally to achieve their desired ends. Critics have argued that actors can be influenced by emotions, biases, and their cultural environment, which can lead them to make irrational decisions.[88] In my view, however, such behavior does not necessarily contradict the principles of strategic theory. The concept of rationality does not imply that the actor always makes the right decisions or that their choices always move them towards their desired ends. Rather, the theory assumes that actors simply make a cost-benefit calculation that informs their decision-making.[89] Although this presupposition cannot be empirically proven, it remains a fundamental tenet of strategic theory and is essential for the functioning of its analytical framework.

F. Definitions of Terms

This thesis uses the following basic terms and definitions:

---

[88] Miles Kahler. "Rationality in International Relations." *International Organization* 52, no. 4 (1998): 919–41. Accessed March 7, 2023. http://www.jstor.org/stable/2601362
[89] Smith, "Strategic Theory…"

cyberattack – Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.[90]

cybersecurity – This thesis follows the Russian government's definition of cybersecurity, which is "a set of conditions under which all components of cyberspace are protected from the maximum possible number of threats and impacts with undesirable consequences."[91] It should be noted, however, that, while the U.S. and its allies focus on assuring cybersecurity, Russia does not distinguish it from the broader concept of information security and does not use the term "cybersecurity" in most of its official documents.

cyberspace – This thesis follows the Russian government's definition of cyberspace as "a sphere of activity in the information space, formed by a combination of communication channels of the Internet and other telecommunication networks, the technological infrastructure that ensures their functioning, and any forms of human activity (individual, organization, state) carried out through their use."[92]

cyberspace capability – A device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.[93]

electronic warfare (EW) – A type of armed struggle, during which radio emissions (radio interference) are exposed to the radio-electronic means of enemy

---

[90] National Institute of Standards and Technology (NIST) Glossary, s.v. "cyber attack." Computer Security Resource Center (CSRC). Accessed February 5, 2022. https://csrc.nist.gov/glossary/term/Cyber_Attack

[91] Federation Council of the Federal Assembly of the Russian Federation. *Cyber Security Strategy Concept of the Russian Federation*. November 29, 2013. Accessed October 20, 2022. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

[92] *Cyber Security Strategy Concept…*

[93] National Institute of Standards and Technology (NIST) Glossary, s.v. "cyberspace capability." Computer Security Resource Center (CSRC). Accessed February 5, 2022. https://csrc.nist.gov/glossary/term/cyberspace_capability

control, communication, and reconnaissance system to change the quality of military information circulating in them, protect their systems from similar effects, as well as change the conditions (environment properties) of radio wave propagation.[94]

information confrontation (informatsionnoe protivoborstvo or Ipb) – The Russian Ministry of Defense defines information confrontation as a type of counter-struggle (between governments, socio-political movements and organizations, military forces, etc.) where each side tries to win (or deal damage) by influencing the adversary's information sphere while protecting its own objects from similar influence.[95] The term "information confrontation" is often used in discussions regarding Russia's hostile activities in cyberspace.

information infrastructure (referring to Russia) – A combination of informatization objects, information systems, internet websites, and communication networks located in the territory of the Russian Federation, as well as in the territories under the jurisdiction of the Russian Federation or used under international treaties signed by the Russian Federation.[96]

information security (*InfoSec*) – This thesis follows the Russian government's interpretation of the term as "the state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity, and sustainable socio-

---

[94] *Dictionary of Terms*, s.v. "Radioelektronnaya borba (REB) [Radio electronic struggle]." Ministry of Defense of the Russian Federation. Accessed October 22, 2022. https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14416@morfDictionary

[95] *Dictionary of Terms*, s.v. "Informatsionnoe protivoborstvo [Information confrontation]." Ministry of Defense of the Russian Federation. Accessed February 5, 2022. http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary

[96] *Doctrine of Information Security…*

economic development of the Russian Federation, as well as defence and security of the State."[97]

information space – A scope of activities associated with the formation, creation, transformation, transmission, usage, storage of information which influences the individual and community awareness, information infrastructure and information itself."[98]

information sphere – A combination of information, informatization objects, information systems, and websites within the information and telecommunications network of the internet, communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere.[99]

information technologies (IT) – Processes, methods for searching, collecting, storing, processing, providing, disseminating information, and methods for implementing such processes and methods.[100]

information warfare (IW) – The confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes, and resources, critical and other structures, undermining the political, economic, and social systems, a massive psychological manipulation of the population to

---

[97] *Doctrine of Information Security of the Russian Federation*. Ministry of Foreign Affairs of the Russian Federation. December 5, 2016. Accessed October 22, 2022. https://publicintelligence.net/ru-information-security-2016/
[98] *Information Space Activities Concept…*
[99] *Doctrine of Information Security…*
[100] *Dictionary of Terms*, s.v. "Informatsionnye tehnologii [Information technologies]." Ministry of Defense of the Russian Federation. Accessed October 22, 2022. https://dictionary.mil.ru/folder/123100/letter/9/

destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force.[101]

information weapons – Information technologies, means, and methods used to conduct information warfare.[102]

national cybersecurity strategy (NCSS) – A high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe.[103]

national interests – Objectively significant requirements of the individual, society, and the state with regard to ensuring their protection and sustainable development.[104]

national security – The state of protection of the individual, society, and the State against internal and external threats in the process of which the exercise of the constitutional rights and freedoms of citizens, a decent quality of life and standard of living for them, sovereignty, independence, state and territorial integrity, and sustainable socioeconomic development are ensured. National security includes the country's defense and all types of security, primarily state, public, informational, environmental, economic, transportation, energy security, and individual security.[105]

national security threat – The set of conditions and factors creating a direct or indirect possibility of harm to national interests.[106]

---

[101] *Information Space Activities Concept…*
[102] *Information Space Activities Concept…*
[103] European Union Agency for Cybersecurity. National Cybersecurity Strategies. Accessed July 28, 2022. https://www.enisa.europa.eu/topics/national-cyber-security-strategies
[104] *Strategy of National Security (*2015)…
[105] *Strategy of National Security (2015)…*
[106] *Strategy of National Security (2015)…*

ransomware – Malware that requires the victim to pay a ransom to access encrypted files.[107]

soft power – The use of a country's cultural and economic influence to persuade other countries to do something, rather than the use of military power.[108]

strategy – This thesis defines strategy as the art and science of developing and using the political, economic, social-psychological, and military powers of the state in accordance with policy guidance to create effects that protect or advance national interests relative to other states, actors, or circumstances.[109]

This chapter introduced the idea behind this thesis along with its research question: *do Russia's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain?* It examined the genesis and evolution of Russia's approach to information security from the seventeenth century to 2021 and provided a succinct overview of some of the prominent literature on the subject. This chapter also highlighted the distinctive characteristics of the Kremlin's approach to InfoSec, including its focus on protecting all media used to transmit and share information, as well as its distinction between information-technical and information-psychological operations. Russia's long history of using information warfare means to achieve its strategic ends, both domestically and internationally was also explored. Finally, this chapter described the theoretical and methodological frameworks

---

[107] Merriam-Webster, s.v. "Ransomware." *Merriam-Webster.com dictionary*. Accessed February 5, 2022. https://www.merriam-webster.com/dictionary/ransomware

[108] *Cambridge University Press*, s.v. "soft power." Cambridge Advanced Learner's Dictionary & Thesaurus. Cambridge University Press, n.d. Accessed February 4, 2022. https://dictionary.cambridge.org/dictionary/english/soft-power

[109] Yarger, *Strategic Theory…*

that will be used to answer the research question and provided definitions of key terms used in this thesis. The next chapter reviews key statements pertaining to InfoSec made in Russia's doctrinal documents to identify the *ends, ways*, and *means* of Russia’s stated information security in the research period.

Chapter II.

Words: Russia's Information Security Strategy on Paper

To gain an understanding of the *ends, ways,* and *means* of Russia's stated information security strategy, this chapter will examine those of the country's main doctrinal documents, which included significant language on InfoSec in the research period. These documents are as follows:

- *Russian Federation Armed Forces' Information Space Activities Concept* of 2011
- *The Military Doctrine of The Russian Federation* of 2014
- *The Strategies of National Security of the Russian Federation* of 2015 and 2021
- *Doctrine of Information Security of the Russian Federation* of 2016
- *Foreign Policy Concepts of the Russian Federation* of 2013 and 2016

These documents communicate Russia's position on a variety of issues, however, for the purposes of this study, my analysis will focus primarily on areas pertaining to the information domain. I will then identify key themes that are consistently reiterated throughout the examined documents and construct a broad outline of Russia's stated information security strategy. The chapter will end with a summary of the main takeaways and testable propositions regarding Russia's expected behavior and resource allocation decisions.

A. The Russian Federation Armed Forces' Information Space Activities Concept of 2011

In 2011, Russia's Ministry of Defense published a document, entitled the *Russian Federation Armed Forces' Information Space Activities Concept* (the *Concept*).[110] The document, which represented Russia's first official doctrinal statement on information security, outlines basic principles, rules, and confidence-building measures, which the Russian military plans to adhere to in order to accomplish its desired ends. Strengthening Russia's defensive capacity, maximizing its ability to prevent and contain conflicts in the information space, and shaping the international information security (IIS) system "for the sake of the world community" are among the *Concept's* main listed objectives, while the growing role of IW and the cross-border effects of information weapons are highlighted as primary challenges. The *Concept* is significant as it is Russia's first official doctrinal statement of this kind.

The document views the information space as a military domain along with the more traditional land, sea, and air, as well as the somewhat more novel outer space. It states that the Russian military can use "all available assets to effectively address the challenges they face."[111] Such assets include "the staff and field intelligence efforts, operational deception, electronic warfare, communications, code and automated C2 [command and control], information work of HQs [headquarters], as well as protection of friendly information systems against electronic, cyber and other threats."[112]

However, the *Concept* makes no specific references to offensive cyber activities by the Russian military. Instead, it states that the Russian Federation faces a "serious threat coming from the global information space."[113] In response to this threat, according

[110] See: *Information Space Activities Concept…*
[111] *Information Space Activities Concept…* Section 2.3.
[112] *Information Space Activities Concept…* Section 2.3.
[113] *Information Space Activities Concept…* Section 1.

to the document, Russia’s Armed Forces have developed mechanisms for deterring, preventing, and resolving armed conflicts in cyberspace. Thus, the *Concept* establishes that the main threats to Russia’s information security are external in nature and come primarily from other countries that develop their own IW concepts to disrupt and gain access to the information spheres of other states.

The document outlines six principles (or fundamental beliefs) that are meant to guide the Russian military's decision-making and behavior in the information space. The principles include the rule of law, priority, complexity, interaction, cooperation, and innovation. For example, as part of the priority principle, the Russian military is required, “as a matter of priority,” to collect timely information about cyber threats and respond with defensive countermeasures.[114] The cooperation principle underscores the importance of coordination between friendly states and international organizations. At the global level, Russia’s goal behind developing cooperation is to establish an “international legal regime” that would regulate state military activities in the information space.[115] At the regional level, Russia plans to use cooperation as a way to establish joint systems “for detection, warning and combating hostile IT acts seen as a threat to peace and security.”[116] The document also calls for increased regional cooperation as a means for regulating and settling regional disputes stemming from hostile uses of IT while utilizing cross-border information systems for confidence building among regional states. As for the innovation principle, it requires the Russian military to leverage the country’s

[114] *Information Space Activities Concept…* Section 2.2.
[115] *Information Space Activities Concept…* Section 2.5.
[116] *Information Space Activities Concept…* Section 2.5.

scientific and manufacturing potential to create advanced cyberspace technologies as well as skilled personnel that could use them.[117]

The *Concept* also outlines the Russian Armed Forces' rules for containment, prevention, and settlement of military conflicts in the information space, as well as some confidence-building measures. It says that the Russian Armed Forces will

> "strive for the maximum exploitation of the information space potential in order to strengthen the defensive capacity of this country, to contain and prevent military conflicts, to develop military cooperation and shape an international information security system for the sake of the world community."[118]

This includes cooperation with the member countries of the Collective Security Treaty Organization (CSTO), the Commonwealth of Independent States (CIS), and the Shanghai Cooperation Organization (SCO). The Russian Armed Forces would also commit to implementing an international cyberspace security treaty under the auspices of the United Nations (UN), in order to extend the existing norms in cyberspace. The document does not offer further details about the proposed treaty.

Thus, we can conclude that, according to the *Concept*, Russia declares the main cyberspace threats to be external; it projects a defensive posture and proposes addressing cybersecurity challenges through the creation of advanced cyberspace technologies, training skilled personnel, and promotion of international laws regulating military activities in cyberspace. It should be noted, however, that, although the document does not mention the possibility of offensive cyberspace actions by the Russian military, its military leadership has often sent a different message. For instance, at a conference of the Russian Academy of Military Sciences in Moscow that took place in January 2012,

---

[117] *Information Space Activities Concept…* Section 2.6.
[118] *Information Space Activities Concept…* Section 5.

shortly after the release of the *Concept*, then-chief of the General Staff Nikolai Makarov reported on the readiness of the Russian Armed Forces to create special units, including what he called "Cyber Command," that would operate in three main areas:

1. Disrupting the adversary's information systems, including the introduction of malicious software;
2. Defending Russia's own communications and control systems;
3. Influencing domestic and foreign public opinion through the media and the internet.[119]

Later that same year, Makarov was replaced by Valery Gerasimov at the helm of the Russian General Staff. Gerasimov continued to stress the importance of cyberspace operations in achieving Russia's strategic goals.

B. The Military Doctrine of the Russian Federation of 2014

Three years after the publication of the *Information Space Activities Concept,* Russia released a new version of its military doctrine (the *Doctrine*). The text outlines the major points of the Russian military policy and resource allocations based on the identified military risks and threats facing the nation.

From the beginning, the *Doctrine* underscores the ongoing redistribution of power "in favour of new centres of economic growth and political attraction."[120] However, it paints an alarming picture when it comes to the risks and threats facing the Russian

[119] "Rossiya: odna armiya i tri mneniya [Russia: One Army and Three Opinions]." *Soldaty RF [Soldiers RF]*. May 3, 2012. Accessed April 9, 2022. https://www.soldati-russian.ru/news/rossija_odna_armija_i_tri_mnenija/2012-03-05-1408
[120] *Military Doctrine…*

Federation. It talks about regional conflicts, the rise of global competition, and interstate rivalry over moral values and models of development. The document states that, while there is a continuing tendency to resolve regional conflicts with the use of force, Russia is not provided with equal security under the existing international security regime.[121] At the same time, the number of military risks and threats Russia encounters is increasing, with many of them now coming from the information space.[122]

It is worth pointing out here that the *Doctrine* distinguishes military risks from threats by the degree of danger they present. The *Russian Military Doctrine* defines military risks as situations that can develop into military threats under certain conditions. In turn, military threats are situations that present a real possibility of military conflict, where opposing sides are ready to resort to the use of military force.[123]

Among the main external military risks, the *Doctrine* lists the build-up and expansion of NATO near Russian borders**,** the deployment of strategic missile defense systems and military units by foreign nations within states and waters bordering on Russia, as well as territorial claims made against Russia and its allies. Besides the traditional military domains, the document also emphasizes risks coming from the intention of other states to place weapons in outer space and the use of information technologies to undermine Russia's sovereignty, political and regional stability.[124]

Regarding military threats, the *Doctrine* expresses Moscow's concern with potential sabotage and military posturing by foreign nations near Russia's borders. It warns of the potential impediment of military command and control functions, the

---

[121] *Military Doctrine*… Article II, Section 10.
[122] *Military Doctrine*… Article II, Section 11.
[123] *Military Doctrine*… Article I, Section 8, Clauses b), c).
[124] *Military Doctrine*… Article II, Section 12.

disruption of Russia's nuclear forces and missile warning systems, as well as nuclear, chemical, and other potentially dangerous facilities. Underscoring the Kremlin's wariness of the expansion of NATO, the *Doctrine* considers the "demonstration of military force in the course of exercises in the territories of states contiguous with the Russian Federation or its allies" as one of the main military threats facing the nation.[125]

Internally, Russia's main military risks are represented by domestic activities aiming at changing Russia's constitutional system, and destabilizing its political order, and information infrastructure. Here again, the text underscores the role of information warfare by mentioning "subversive information activities against the population, especially young citizens of the State, aimed at undermining historical, spiritual, and patriotic traditions related to the defense of the Motherland."[126]

Russia's increasing focus on the information sphere is further emphasized in the description of the characteristic features of modern military conflicts. The *Doctrine* notes that informational, political, economic, and other non-military measures are widely used to incite protests within the population of the targeted state.[127] Electronic warfare and other non-military measures, along with more traditional weapons, are employed to exert "simultaneous pressure on the enemy throughout the enemy's territory in the global information space, airspace and outer space, on land and sea."[128] In a more conspiratorial tone, the document notes the employment of political actors and public associations

[125] *Military Doctrine*... Article II, Section 14, Clauses b), d).
[126] *Military Doctrine*... Article II, Section 13, Clause c).
[127] *Military Doctrine*... Article II, Section 15, Clause a).
[128] *Military Doctrine*... Article II, Section 15, Clause c).

funded and directed from abroad in order to destabilize the situation within the enemy's territory.[129]

To address these challenges and deter military conflicts, the *Doctrine* sets the task of employing "modern technical means and information technologies" in order to assess and forecast global military and political developments.[130] It also tasks the government with the use of non-military means for neutralizing potential military risks and threats.[131] Additionally, the *Doctrine* aims to create conditions that would reduce the risk posed by the illegal use of information technologies with the intent to undermine national sovereignty, as well as international and regional stability.[132] This could indicate the Kremlin's intentions to establish stricter regulatory and monitoring measures over the Russian information space.

In sum, many of the proposed policy actions outlined in the document show Moscow's clear intentions to better arm itself against the perceived threats coming from the information sphere. The *Doctrine,* however, does not describe the Russian Armed Forces' strategy for operating in cyberspace. Still, given the risks, threats, and proposed policy actions stated in the *Doctrine*, I can conclude that the Kremlin considers InfoSec and IW readiness as integral parts of its military strategy.

Overall, Russia's 2014 *Military Doctrine* is primarily defensive in tone. Just like the 2011 *Information Activities Concept*, it focuses primarily on external risks and threats and emphasizes the need to develop Russia's technological capabilities to better prepare itself for modern military conflicts where opposing sides increasingly use non-military

[129] *Military Doctrine…* Article II, Section 15, Clause j).
[130] *Military Doctrine…* Article III, Section 21, Clause a).
[131] *Military Doctrine…* Article III, Section 21, Clause b).
[132] *Military Doctrine…* Article III, Section 21, Clause s).

measures in order to gain a strategic advantage. When compared to its predecessor, however, the 2014 draft shows a significant change in its tone and the message it sends to the West. Although Russia's 2010 *Military Doctrine* still perceived NATO and the Western block as potential opponents, it declared willingness to consider their interests as long as they were consistent with Russia's own national interests. Such an approach demonstrated Moscow's intentions to coexist with other powerful players in the global geopolitical arena.[133] The 2010 document even mentioned Russia's willingness to work with NATO to "strengthen the system of collective security."[134] There is no such language in the 2014 draft.

Also, new to the 2014 document are the emphases on information warfare, Western military meddling near Russia's borders, and the threat of undermining its territorial sovereignty. Thus, we can see a clear escalation in hostile rhetoric between the 2010 and 2014 drafts. Russia's 2014 *Military Doctrine* clearly defines NATO as its main geopolitical opponent, bringing the overall dynamic between Russia and the West closer to that of the Cold War era.

C. Strategies of National Security of the Russian Federation of 2015 and 2021

On December 31, 2015, Russian President Vladimir Putin approved a new *Strategy of National Security* (the *NS Strategy*). The document outlines Russia's strategic

[133] Nina Samarkina. "Strategii I Proekty Razvitiya Sovremennogo Oboronnogo Sectora RF [Strategies and Projects for the Development of a Modern Defense Sector of the Russian Federation]." *Vestnik RGGU*. Series: Political Science. History. International relations. Foreign area studies. Orientalism, 7, pages 21 – 28. (2014). Accessed July 30, 2022. https://elibrary.ru/item.asp?id=21769543
[134] *Military Doctrine (2010)...* Article III, Section 18, Clause e).

interests, priorities, and objectives, as well as foreign and domestic policy goals aimed at ensuring national security and sustainable development.[135]

The *NS Strategy* starts by noting positive trends in Russia's growing population, and economy, improved public health, and strengthening spiritual and moral values among its citizens.[136] It talks about Russia's increasing role in "resolving the most important international problems, settling military conflicts, and ensuring strategic stability and the supremacy of international law in interstate relations."[137] However, the text immediately contrasts these accomplishments with the surge of new national security threats posed by the U.S. and its allies "who are seeking to retain their dominance in world affairs."[138] According to the document, the West tries to contain Russia by pressuring it in the spheres of politics, economy, military, and information.[139]

Similar to the 2014 *Military Doctrine*, the 2015 *NS Strategy* portrays Russia as a victim of an inequitable international security arrangement and attacks NATO for building up its military capabilities near Russian borders.[140] It blames both the U.S. and EU for supporting the 2014 Revolution of Dignity (Maidan Revolution) in Ukraine, which, as the document claims, led to a socioeconomic crisis and the rise of the far-right nationalism in Ukraine, turning it into "a chronic seat of instability in Europe and in the immediate vicinity of Russia's borders."[141] Much of that support is perceived to have happened in the information arena, as the document notes an increase in attempts by some countries to use information technologies to falsify history and manipulate public

---

[135] *Strategy of National Security (2015)…* Article I.
[136] *Strategy of National Security (2015)*... Article II, Sections 9, 10, 11.
[137] *Strategy of National Security (2015)*... Article II, Section 8.
[138] *Strategy of National Security (2015)*... Article II, Section 12.
[139] *Strategy of National Security (2015)*... Article II, Section 12.
[140] *Strategy of National Security (2015)*... Article II, Section 14.
[141] *Strategy of National Security (2015)*... Article II, Section 17.

opinion to accomplish their geopolitical objectives.[142] The text declares that, as a result of these processes, the international arena is now characterized by the intensifying global information confrontation (rus.: *informatsionnoe protivoborstvo)*.

Among the main information-related threats to state and public security, the *NS Strategy* lists intelligence activities conducted by foreign states, activities by terrorist and criminal groups, and activities that leverage ITs in order to promote extremist ideologies, and separatism, and to undermine Russia's political order.[143] Also perceived as a threat is "external cultural and information expansion" in the form of western popular culture that weakens the unity of the Russian people and leads to the erosion of Russia's traditional moral and spiritual values.[144] The emphasis on moral and spiritual values is particularly notable and consistent throughout the document. In fact, it counts more than a dozen such references.

To address these threats, the *NS Strategy* aims at better unifying Russian society around the aforementioned moral and spiritual values, modernizing the economy, and improving the country's defensive capabilities.[145] Particularly, it talks about improving the system for identifying information threats and taking measures to protect Russian citizens from the destructive influence of the information spread by "extremist and terrorist organizations, foreign special services and propaganda structures."[146] The document does not specify the nature of these protective measures, but it would not be too farfetched to infer that such measures would likely come at the cost of restricting the

---

[142] *Strategy of National Security (2015)*… Article II, Section 21.
[143] *Strategy of National Security (2015)*… Article II, Section 43.
[144] *Strategy of National Security (2015)*… Article II, Section 79.
[145] *Strategy of National Security (2015)*… Article II, Section 26.
[146] *Strategy of National Security (2015)*… Article II, Section 26.

free flow of information within the Russian territory through harsher laws and/or increased censorship. Another way Russia plans to counter the outlined threats is by creating an information infrastructure that would allow Russian citizens to receive better access to information on relevant issues, including "society's sociopolitical, economic, and spiritual life," according to the document.[147] This includes the creation of "cinematographic and printed output, television and radio programs, and Internet resources" that would also be broadcast over the territories of the Commonwealth of Independent States (CIS) and contiguous regions.[148]

The *NS Strategy* also highlights Russia's dependence on imported technologies, including computer software and hardware, as factors negatively affecting national security.[149] To counter these factors, it calls for "the raising of the level of technological security, including in the information sphere."[150] Russia aims to accomplish this through the development of the high-tech sector by stimulating private businesses and creating business incubators and techno-parks that could produce technology-based goods and services for state-owned companies.

Another objective to that end is improving the existing state system for training qualified specialists and workers, as well as prioritizing the development of basic and applied science and education.[151] All this, in turn, would stimulate the Russian economy while providing the technological innovation necessary for the development of modern military and information infrastructures ensuring national security.[152] Such phrasing

---

147 *Strategy of National Security (2015)*... Article II, Section 53.
148 *Strategy of National Security (2015)*... Article II, Section 82.
149 *Strategy of National Security (2015)*... Article II, Section 68.
150 *Strategy of National Security (2015)*... Article II, Section 69.
151 *Strategy of National Security (2015)*... Article II, Section 69.
152 *Strategy of National Security (2015)*... Article II, Section 62.

indicates that the Russian State continues to see the military-industrial complex as one of the main drivers of technological innovation.

In the international arena, Russia plans to pursue its national security interests by relying on international law and principles of mutual noninterference in the domestic affairs of other states, according to the document.[153] The strategy also calls for the development of the Collective Security Treaty Organization (CSTO) as an international organization that can address regional threats both in the military and information domains.[154] Finally, the *NS Strategy* highlights what it describes as Russia's role in preserving strategic stability by contributing to the development of the IIS system – a message that has been consistently emphasized in both the 2011 *Armed forces' Information Space Activities Concept* and the 2014 *Military Doctrine.*[155]

Despite its somewhat vitriolic tone, Russia's 2015 *NS Strategy* proclaims an overall defensive and non-combative approach to averting its perceived security risks and threats. It says Russia will seek to avoid an arms race and instead pursue "an open, rational, and pragmatic foreign policy ruling out costly confrontation."[156] Prioritizing economic cooperation, multilateral trade, and diplomacy, the *NS Strategy* reserves the use of military force only when all other nonviolent means have been exhausted.[157]

The Kremlin changed that narrative in the 2021 edition of the *NS Strategy*. Significantly escalating its rhetoric, the new document claims that "space and information

[153] *Strategy of National Security (2015)*… Article II, Section 87.
[154] *Strategy of National Security (2015)*… Article II, Section 90.
[155] *Strategy of National Security (2015)*… Article II, Section 104.
[156] *Strategy of National Security (2015)*… Article II, Section 27.
[157] *Strategy of National Security (2015)*… Article II, Sections 28, 29.

space are being actively explored as new spheres of warfare."[158] It says that special services and armed forces of foreign states are utilizing the information environment to conduct reconnaissance operations and rehearse sabotaging Russia's critical infrastructure facilities.[159] Underscoring the importance of the subject matter, the updated document features an entire section dedicated to information security.

While Russia expressed concerns about the damaging influence of western pop culture in the 2015 draft of the *NS Strategy*, the 2021 version takes a much more confrontational tone by calling it an "information and psychological sabotage" that threatens Russia's "cultural sovereignty."[160] The document also lays out a number of Russia's information-related grievances toward the West:

> "Information campaigns are carried out to form a hostile image of Russia. The use of the Russian language is restricted, the activities of Russian mass media and the use of Russian information resources are banned, and sanctions are imposed on Russian athletes. The Russian Federation is unreasonably accused of violating international obligations, conducting computer attacks, and interfering in the internal affairs of foreign states."[161]

The Kremlin further laments that, while Russia's information resources are being increasingly targeted from abroad, its initiatives to improve international information security "meet resistance from foreign states seeking to dominate the global information space."[162] In addition to foreign governments, Russia also accuses transnational

[158] *Strategy of National Security of the Russian Federation*. Ministry of Defense of the Russian Federation. July 2, 2021. Article II, Section 17. Accessed November 7, 2022. https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf
[159] *Strategy of National Security (2021)…* Article IV, Section 51.
[160] *Strategy of National Security (2021)…* Article IV, Section 88.
[161] *Strategy of National Security (2021)…* Article II, Section 19.
[162] *Strategy of National Security (2021)…* Article IV, Section 50.

corporations of trying to monopolize the internet and manipulate information for political reasons.[163]

While the 2015 *NS Strategy* assumed a largely defensive posture, the new version of this strategy talks about offensive measures and proposes, among other things, the "development of forces and means of information confrontation."[164] Borrowing from the 2014 *Military Doctrine*, the 2021 *NS Strategy* also discusses the need to develop a new system for "forecasting, identifying and preventing threats to the information security of the Russian Federation."[165] References to artificial intelligence and quantum computing as a means of strengthening Russia's InfoSec constitute another innovation in the 2021 document.[166]

In sum, both the 2015 and 2021 versions of Russia's national security strategy express the government's acute concerns with what it sees as growing threats to Russia's information security. Both drafts also clearly point to the West as the source of what the Kremlin sees as malicious information operations aimed at destabilizing Russia's political regime and its national security. Overall, the 2021 document takes a markedly more aggressive stance toward the West than its predecessor. The 2021 version of the strategy also introduces several offensive-oriented approaches to dealing with Russia's perceived information threats.

---

[163] *Strategy of National Security (2021)…* Article IV, Sections 44, 53.
[164] *Strategy of National Security (2021)…* Article IV, Section 57, Clause 10).
[165] *Strategy of National Security (2021)…* Article IV, Section 57, Clause 2). Similarly, Russia's 2014 *Military Doctrine* established as one of Russia's main tasks "to assess and forecast the development of the military and political situation at global and regional levels, as well as the state of interstate relations in the military-political field with the use of modern technical means and information technologies." *See: Military Doctrine…* Article III, Section 21, Clause a).
[166] *Strategy of National Security (2021)…* Article IV, Section 57, Clause 12).

D. Doctrine of Information Security of the Russian Federation of 2016

On December 6, 2016, Vladimir Putin signed the new *Doctrine of Information Security of the Russian Federation* (the *InfoSec Doctrine*) that replaced the one adopted in 2000. While Russia does not have a dedicated publicly released national cyberspace strategy, this document represents its closest approximation. The doctrine states the government's official views on ensuring Russia's national security in cyberspace, as well as the wider information environment. It outlines the "strategic objectives and key areas of InfoSec taking into account the strategic national priorities of the Russian Federation."[167] Continuing the tone of the preceding documents, the *InfoSec Doctrine* emphasizes the growing threat posed to Russia in the information space by other states.

On the surface, the *InfoSec Doctrine* seems to aspire to many of the same democratic goals commonly used by Western states, such as "ensuring and protecting constitutional human and civil rights and freedoms with regard to the receipt and use of information, privacy in the use of information technologies, [and] providing information support to democratic institutions."[168] However, a deeper analysis of the document reveals that it is diverging from key Western concepts, while increasingly drawing on Soviet-era narratives.

The majority of the information threats highlighted in the document are stated to emanate primarily from foreign actors, seeking to undermine the social values and stability of the Russian state. Some of these threats include the use of the transboundary flow of information for geopolitical goals, as well as the buildup of IT capabilities by

[167] *Doctrine of Information Security*… General Provisions, 3.
[168] *Doctrine of Information Security*… Article II, Section 8, Clause a).

other states with the purpose of using them for military goals.[169] The "other states" are not named, but one state that fits this description is the U.S. whose doctrinal documents include overt references to carrying out offensive cyber operations. For example, in his 2011 memorandum to secretaries of the military departments, the U.S. Secretary of Defense Robert Gates characterized information operations as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."[170]

Another threat listed in the *InfoSec Doctrine* that reads as a likely reference to the U.S. is "the desire of individual States to use their technological superiority to dominate the information space."[171] Indeed, global internet governance has been an increasingly contentious issue in recent decades.[172] The U.S. government historically controlled the Internet Assigned Numbers Authority (IANA), the body that manages the web's domain name system (DNS) and other internet protocol-related symbols and numbers. Although the nonprofit Internet Corporation for Assigned Names and Numbers (ICANN) was officially tasked with managing IANA, the U.S. Department of Commerce (through the U.S. National Telecommunications & Information Administration (NTIA)) had the ability to overrule any decisions made by ICANN.

---

[169] *Doctrine of Information Security…* Article III, Sections 10, 11.
[170] The U.S. Secretary of Defense. *Strategic Communication and Information Operations in the DOD*. Memorandum. January 25, 2011. Accessed July 30, 2022. http://www.ecrow.org/assets/osd%2012401-10.pdf
[171] *Doctrine of Information Security…* Article III, Section 19.
[172] H. M. Haugen. "The crucial and contested global public good: principles and goals in global internet governance." *Internet Policy Review*, 9(1). 2020. Accessed July 30, 2022. https://doi.org/10.14763/2020.1.1447

On October 1, 2016, the U.S. government fully transferred control over IANA to ICANN whose governing body is composed of multiple international stakeholders from government organizations, private companies, and individual internet users.[173] Nevertheless, the current private-sector-based internet governance regime remains fundamentally at odds with the Russian government's views on national cyberspace sovereignty.[174] As such, Russia's *InfoSec Doctrine* prioritizes the development of a national system for managing Runet.[175]

In line with the previously reviewed documents, the *InfoSec Doctrine* emphasizes the need to create international legal norms regulating interstate relations in cyberspace. The document lists "promoting in international organizations the position of the Russian Federation" as one of the government's top objectives.[176] This could serve as an indicator of Moscow's intentions to continue pushing for international regulation of cyberspace at the state level.

Another characteristic feature of the Russian *InfoSec Doctrine* is that it offers a more comprehensive definition of the information sphere than its predecessors. For instance, one of the perceived threats mentioned in the document discusses foreign intelligence services that increasingly use "information and psychological tools with a view to destabilizing the internal political and social situation in various regions across the world, undermining the sovereignty and violating the territorial integrity of other

---

[173] "Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends." Internet Corporation for Assigned Names and Numbers (ICANN). October 1, 2016. Accessed July 30, 2022. https://go.icann.org/3Icty8D; Also see Robert Sanders. "The U.S. government no longer controls the internet." *Business Insider*. October 4, 2016. Accessed July 30, 2022. https://www.businessinsider.com/the-us-government-no-longer-controls-the-internet-2016-10

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

[175] *Doctrine of Information Security…* Article IV, Section 29, Clause e).

[176] *Doctrine of Information Security…* Article IV, Section 29, Clause d).

States."[177] The underlying concept behind this statement points to the recognition by the Russian government of how information tools (as part of information-psychological operations) can be used to impact entire societies.

The document also highlights the Russian authorities' concern with foreign media circulating "biased assessments of State policy of the Russian Federation."[178] Again, the underlying assumption here is that mass media are serving as an extension of the government to help accomplish its strategic geopolitical goals. In Moscow's perception, any society, be it foreign or domestic, is but a subject of manipulation by the state. Therefore, it should not be surprising that the Kremlin sees every anti-government expression, be it the color revolutions or anti-Putin protests of 2011-2012 in Russia, as an event orchestrated from the top down by forming a desired public sentiment. As such, the Kremlin perceives cyberspace and independent media to be presenting a direct threat to Russia's established regime.

The doctrine deals with such issues by outlining among its national interests the provision of "the Russian and international community with reliable information on the State policy of the Russian Federation and its official position on socially significant events in Russia and in the world, and applying information technologies to ensure the national security of the Russian Federation in the sphere of culture."[179] In other terms, the document hints at Russia's intentions to use mass media for shaping public opinion in a way favorable to the government.

[177] *Doctrine of Information Security…* Article III, Section 12.
[178] *Doctrine of Information Security…* Article III, Section 12.
[179] *Doctrine of Information Security…* Article II, Section 8, Clause d).

Among Russia's top InfoSec priorities, the doctrine states: "suppressing the activity detrimental to the national security of the Russian Federation, carried out by special services and organizations of foreign States as well as by individuals using technical means and information technologies."[180] Such strong emphasis on the malignant influence of foreign states clearly indicates the Kremlin's growing insecurity in the information domain. This rhetoric can also be a sign of potential future clampdowns on NGOs and other foreign agents operating on Russia's territory, as well as establishing stricter control over the Russian information space.

When it comes to Russian citizens, the *InfoSec Doctrine* talks about the need to maintain "a balance" between their rights to the free exchange of information and restrictions necessary to ensure national security in the information sphere.[181] The text also highlights the need for "constant monitoring" of information threats.[182] This further indicates the Kremlin's possible intentions to tighten its grip over the Russian segment of the internet under the guise of defending national security against external threats.

Among other threats highlighted in the *InfoSec Doctrine*, are Russia's dependence on foreign software and hardware components for its telecommunications equipment, as well as the shortage of qualified personnel in the Infosec sphere. To address these challenges, the document puts the goal of growing the domestic IT sector on the list of Russia's national interests in the information sphere.

Overall, based on the examined statements made in Russia's 2016 *InfoSec Doctrine,* I can conclude that Moscow once again projects a defensive posture in the

---

[180] *Doctrine of Information Security…* Article IV, Section 23, Clause b).
[181] *Doctrine of Information Security…* Article V, Section 34, Clause c).
[182] *Doctrine of Information Security…* Article V, Section 34, clause d).

global information sphere. It portrays itself to be under constant information attack by the West. Most of the actions proposed to defend or advance Russia's *InfoSec* interests are focused on countering external threats; balancing against foreign media's biased narratives about Russia's policies; developing the domestic IT sector to produce enhanced InfoSec services; and developing a legal framework for an IIS system.

E. Foreign Policy Concepts of the Russian Federation of 2013 and 2016

In February 2013, the Russian Ministry of Foreign Affairs released a new *Foreign Policy Concept* (the *FP Concept*).[183] It replaced the previous iteration of the document introduced in 2008. The 2013 document represents Russia's vision of priorities and objectives of its foreign policy.

Congruent with Russia's wider security framework, the *FP Concept* directly acknowledges both the *National Security Strategy* and the *Military Doctrine*. The document describes the modern international arena as one of rising tensions where new centers of economic and political power are creating a multipolar international environment.[184] In this evolving landscape, Russia sees "increased responsibility for setting the international agenda and shaping the system of international relations."[185]

Besides economic, legal, scientific, environmental, and demographic factors, the *FP Concept* highlights information technologies as equally important for influencing the international political environment as traditional military power.[186] Acknowledging

---

[183] *Konseptsiya vneshnei politiki Rossiiskoi Federatsii* [*Foreign Policy Concept of the Russian Federation*]. Ministry of Foreign Affairs of the Russian Federation**.** February 12, 2013. Accessed October 30, 2022. https://www.rusemb.org.uk/in1/
[184] *Foreign Policy Concept (2013)…* Article II, Section 6.
[185] *Foreign Policy Concept (2013)…* Article I, Section 3.
[186] *Foreign Policy Concept (2013)…* Article II, Section 10.

political instability in the Middle East and North Africa, Russia expresses its concern with "civilizational fault line clashes" that happen as a result of the competition between varying values and models of economic development.[187] To better compete in this new marketplace of values, the *FP Concept* introduces "soft power" as "an indispensable component of modern international relations."[188] Proposed as an alternative to classical diplomacy, Russia's soft power toolkit would consist of methods and technologies leveraging information, culture, civil society, and other auxiliary elements.

As part of this new soft power strategy, the *Concept* highlights Russia's aim to

> "develop its own effective means of information influence on public opinion abroad, strengthen the role of Russian mass media in the international information environment providing them with essential state support, as well as actively participate in international information cooperation, and take necessary measures to counteract information threats to its sovereignty and security."[189]

A significant emphasis is also placed on widening the space for the Russian language and culture by facilitating learning opportunities and supporting the Russian diaspora abroad.[190] The *FP Concept* specifically notes that new information and communications technologies offer new possibilities for deploying these elements of soft power to help achieve Russia's foreign policy objectives.[191]

On November 30, 2016, President Putin approved an updated version of the Russian *FP Concept*. Compared to its predecessor, the new version notably elevates its focus on InfoSec as a serious transborder threat while also assuming a more negative tone towards the U.S. Similar to the *Military Doctrine* released two years earlier, the 2016 *FP*

---

[187] *Foreign Policy Concept (2013)*... Article II, Sections 13, 14.
[188] *Foreign Policy Concept (2013)*... Article II, Sections 20.
[189] *Foreign Policy Concept (2013)*... Article III, Section 41.
[190] *Foreign Policy Concept (2013)*... Article III, Section 39, Clauses d-f).
[191] *Foreign Policy Concept (2013)*... Article III, Section 41.

Concept blames the traditional Western powers for the growing global and regional instability stemming from their attempts to contain the rise of new centers of power in order to continue shaping the rules of the international system.[192] It calls out the U.S. and its allies for adopting a containment policy against Russia, stating that the "political, economic, information and other pressure Russia is facing from them" is "detrimental to the long-term interests of all sides," and inhibits everyone's ability to address transnational threats facing the international community.[193]

Noting Russia's activities in the global information space among the main objectives of its foreign policy, the 2016 *FP Concept* introduces such terms as "*cyberspace,*" "*cybercrime,*" and "*cybersecurity*." It warns about the growing role of ITs in influencing international politics and the inability of existing military and political alliances to address threats by focusing on securing individual countries in an increasingly interconnected world.[194] Instead, Russia advocates a comprehensive and coordinated effort by members of the UN to better protect the international community from cybercrime and other cross-border challenges.

In its own foreign policy, Russia resolves to take

> "necessary measures to ensure national and international cybersecurity, counter threats to State, economic and social security emanating from cyberspace, combat terrorism and other criminal threats involving the use of information and communication technology; deters their use for military-political aims that run counter to international law, including actions aimed at interfering in the domestic affairs of States or posing a threat to international peace, security and stability; and seeks to devise, under the UN auspices, universal rules of responsible behaviour with

---

[192] *Konseptsiya vneshnei politiki Rossiiskoi Federatsii* [*Foreign Policy Concept of the Russian Federation*]. Ministry of Foreign Affairs of the Russian Federation**.** November 30, 2016. Article II, Section 5. Accessed October 30, 2022. https://www.rusemb.org.uk/rp_insight/
[193] *Foreign Policy Concept (2016)…* Article IV, Section 61.
[194] *Foreign Policy Concept (2016)…* Article II, Sections 7, 8.

> respect to international cyber security, including by rendering the internet governance more international in a fair manner."[195]

The document notes that the Russian government sees potential for increased cooperation with the EU in addressing these challenges.[196] The reference to making internet governance more international is likely made in connection with Russia's continued efforts to promote a new cybersecurity treaty that would replace the current Budapest Convention on Cybercrime implemented by the Council of Europe in 2004 and signed by sixty-six countries.[197] Despite being a member of the Council, Russia refused to sign the Convention, arguing that it would undermine its sovereignty by allowing international law enforcement to open investigations into cybercrimes originating on its territory.[198] The Russian government has since continued to advocate a new treaty.

Similar to the 2013 version, the updated *FP Concept* expresses interest in "building mutually beneficial relationships" with the U.S., saying that the two states have "vast potential in trade and investment, scientific and technical and other types of cooperation."[199] However, this statement is immediately followed by an assertion that Russia finds pressure exerted on it by the U.S. unacceptable and reserves the right to respond by "bolstering of national defence and taking retaliatory or asymmetrical measures."[200]

---

[195] *Foreign Policy Concept (2016)…* Article III, Section 28.
[196] *Foreign Policy Concept (2016)…* Article IV, Section 64.
[197] Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. Council of Europe. Accessed July 30, 2022. https://www.coe.int/en/web/cybercrime/parties-observers
[198] John Markoff and Andrew E. Kramer. "U.S. and Russia Differ on a Treaty for Cyberspace." *The New York Times*. June 27, 2009. Accessed July 30, 2022. https://www.nytimes.com/2009/06/28/world/28cyber.html
[199] *Foreign Policy Concept (2016)…* Article IV, Section 72.
[200] *Foreign Policy Concept (2016)…* Article IV, Section 72.

Overall, the 2016 version of Russia's *FP Concept* appears to be more assertive in its language toward the West than its predecessor. It also adds a new focus on cyberspace and information security. The 2013 version of the document contains only a passing remark about InfoSec, focusing primarily on building Russia's soft power in the information domain by supporting the Russian language, culture, and mass media. The 2016 edition adds the technological aspects of ensuring national and international cybersecurity and raises Russia's InfoSec objectives to the level of national foreign policy priorities.

F. Russia's Stated Information Security Strategy: Key Themes and Propositions

Now that I have reviewed Russia's strategic doctrinal statements pertaining to InfoSec, I will use the analytical method of thematic analysis to summarize the main takeaways and identify key themes that are consistently reiterated throughout the examined doctrines. As stated in Chapter I, thematic analysis is a qualitative research method that involves identifying and analyzing recurring themes or patterns in a set of documents. To help uncover these common InfoSec themes, I have organized my takeaways into four categories: (1) *perceived InfoSec threats;* (2) *opportunities to defend or advance InfoSec interests;* (3) *proposed domestic policy actions; and* (4) *proposed foreign policy actions.*

1. Perceived Information Security Threats

The Kremlin's stated InfoSec strategy is based on the premise that Russia is actively involved in an ongoing information confrontation with the West. This is evidenced by numerous unambiguous statements made in the *Military Doctrine* of 2014, *Strategies of National Security* of 2015 and 2021, and both 2013 and 2016 drafts of the *Foreign Policy Concept*. As the U.S. continues its efforts to preserve a unipolar world by trying to contain Russia, Moscow foresees a period of increased global and regional instability.[201] As such, Russia must be prepared to counter a wide variety of new threats and challenges, many of which are coming from the information space.

Indeed, virtually all of the documents reviewed in this chapter highlight the information space as the source of growing security challenges. The 2013 *Foreign Policy Concept* cites the use of ITs for international terrorism and criminal activities, as well as the unlawful use of "soft power" (which includes information methods and technologies) to exert political pressure on sovereign states as the main threats to its information security.[202] The 2016 version of the concept specifies that the information pressure in question is exerted on Russia by the U.S. and its allies.[203] The two major InfoSec risks identified by the Russian *Military Doctrine* of 2014 are the use of ITs to undermine Russia's sovereignty, political and regional stability, and subversive domestic information activities aimed at undermining historical, spiritual, and patriotic traditions.[204]

The 2011 *Armed Forces' Information Space Activities Concept* doesn't identify specific InfoSec threats, but instead cites the 2000 *Doctrine of Information Security*, saying that states developing their own offensive IW concepts to disrupt information domains of other states are the main source of external threats to Russia's InfoSec. The updated 2016 draft of the *Doctrine of Information Security* adds to the list of threats the

[201] *Foreign Policy Concept (2016)…* Article IV, Section 61.
[202] *Foreign Policy Concept (2013)…* Article II, Section 20, Article III, Section 32, Clause h).
[203] *Foreign Policy Concept (2016)…* Article IV, Section 61.
[204] *Military Doctrine…* Article II, Section 12, Clause l) and Section 13, Clause c).

growing number of computer crimes, “blatant discrimination” of the Russian media abroad, biased assessments of Russian policy by foreign media, and external information pressure that aims to erode Russian traditional spiritual and moral values.[205]

The *National Security Strategy* of 2015 highlights the use of IT by other states to manipulate public opinion and falsify Russian history to achieve their geopolitical goals.[206] It also warns of the decline in the role of the Russian language in the world, as well as the external “cultural and information expansion,” including Western pop culture, that supposedly undermines Russia’s traditional moral and spiritual values.[207] Similarly, the 2021 draft of the *National Security Strategy* highlights the unfair treatment of the Russian language but adds to the list of InfoSec threats the banning of the Russian media, as well as information campaigns conducted to form a hostile image of Russia in the global information sphere.[208] The document also recognizes Russia’s dependence on foreign ITs as a vulnerability for its information resources and critical information infrastructure facilities.[209]

2. Opportunities to Defend or Advance Information Security Interests

Russian authorities believe the information space can both endanger the stability of the ruling regime and serve as a means to defend and advance its security interests. The perceived opportunities to leverage the information space to strengthen Russia’s defensive capacity, shield its people from foreign information influence, and promote

---

[205] *Doctrine of Information Security…* Article III, Section 12, 14
[206] *Strategy of National Security (2015)…* Article II, Section 21
[207] *Strategy of National Security (2015)…* Article IV, Section 79.
[208] *Strategy of National Security (2021)…* Article II, Section 19.
[209] *Strategy of National Security (2021)…* Article IV, Section 55.

Moscow's point of view in the global information space appear as throughlines across most of the reviewed doctrines.

For example, the 2011 *Armed Forces' Information Space Activities Concept* recognizes the opportunity in utilizing information space to strengthen Russia's defensive capacity and leverage Russia's scientific and production potential to create advanced cyberspace technologies.[210] Russia's *Military Doctrine* of 2014 aims to utilize modern ITs to "assess and forecast the development of the military and political situation at global and regional levels, as well as the state of interstate relations in the military-political field."[211] It also talks about using non-military means to neutralize potential military risks and threats.[212]

As it follows from its 2015 *Strategy of National Security*, Russia sees an opportunity in developing its own informational measures (among others) to ensure strategic deterrence and prevent the use of armed force against Russia.[213] It talks about improving its system for identifying and countering threats in the information sphere and taking measures to protect its citizens from the destructive influence of foreign propaganda.[214] Finally, it highlights the opportunity to make the country more technologically independent from the West in the information sphere by improving scientific education and developing public-private partnerships in the sphere of science and technologies.[215] The 2021 draft maintains a similar focus by emphasizing the need to develop a safe information space protecting Russian society from destructive

---

[210] *Information Space Activities Concept…* Section 2.6.
[211] *Military Doctrine…* Article III, Section 21, Clause a).
[212] *Military Doctrine…* Article III, Section 21, Clause b).
[213] *Strategy of National Security (2015)…* Article IV, Section 36.
[214] *Strategy of National Security (2015)…* Article IV, Section 47.
[215] *Strategy of National Security (2015)…* Article IV, Section 69.

psychological impacts and developing information measures aimed at preventing the use of military force against Russia.[216]

The Russian *Doctrine of Information Security* of 2016 aims to counter foreign influence in the information sphere and suppress activity in cyberspace that is detrimental to national security.[217] It also calls for leveraging IT to support the Russian culture and provide both the Russian and international communities with the Kremlin's official point of view on world events.[218] Finally, the document aims to support the development and production of competitive InfoSec products and services.[219] Similar to the *Doctrine of Information Security*, both Russia's 2013 and 2016 *Foreign Policy Concepts* look forward to providing the world with the Russian government's perspective on its domestic and foreign policies, broader international issues, and Russian cultural and scientific achievements.[220]

3. Proposed Domestic Policy Actions

Russia's doctrinal documents outline a number of information risks and threats, as well as opportunities to defend or advance the nation's InfoSec interests. The common themes in the proposed domestic policy actions remain fairly consistent with those outlined in the previous two subsections. They center primarily around such domestic policy actions, as developing the IT industry, training skilled personnel, and securing

---

[216] *Strategy of National Security (2021)…* Article III, Section 3 and Article IV, Section 40, Clause 2).
[217] *Doctrine of Information Security…* Article IV, Section 23, Clause b).
[218] *Doctrine of Information Security…* Article II, Section 8, Clause d).
[219] *Doctrine of Information Security…* Article IV, Section 24.
[220] *Foreign Policy Concept (2013)…* Article III, Section 40; *Foreign Policy Concept (2016)…* Article III, Section 46.

Russia's ICT infrastructure. In addition, they call for promoting Russian content, and the Russian language itself, in the global information space.

For the Russian State to achieve its domestic InfoSec ends, the 2011 *Armed Forces' Information Space Activities Concept* proposes developing an InfoSec system for the Russian military that would enable the use of such means as early detection, prevention, and settlement of cyberspace military conflicts.[221] The document also talks about using the Russian military colleges to train new information space specialists.[222] Russia's *Military Doctrine* of 2014 aims to improve the system of InfoSec of the armed forces by enhancing the capacity and means of IW, as well as by creating conditions that would reduce the risk of using ICT for military-political purposes.[223]

The 2015 *Strategy of National Security* underscores the need to ensure Russia's cultural sovereignty by protecting its society from the destructive information and psychological impacts coming from abroad. This is to be accomplished by establishing better government control in the information sphere.[224] To further counter the foreign information influence, the *Strategy* advocates the creation of state-funded internet resources, movies, print media, television, and radio programs. Additionally, the government would create a common "information-telecommunications medium on the territories of the CIS member states and in contiguous regions."[225]

The 2021 version of the *Strategy* introduced the need for Russia to develop "a system for forecasting, identifying and preventing" InfoSec threats, including critical

---

[221] *Information Space Activities Concept…* Section 3.1.
[222] *Information Space Activities Concept…* Section 2.6.
[223] *Military Doctrine…* Article III, Section 46, Clause c); Section 21, Clause s).
[224] *Strategy of National Security (2015)…* Article II, Section 82.
[225] *Strategy of National Security (2015)…* Article II, Section 82.

information infrastructure facilities. The updated document emphasizes the effective detection and prevention of offenses committed through ICT, as well as increased security, resilience, and freedom from foreign control of the Russian internet and other ICT infrastructure. Finally, it proposes improving InfoSec by using Russian-made ITs, as well as advanced technologies, such as artificial intelligence and quantum computing.[226]

The Russian *Doctrine of Information Security* of 2016 echoes both the 2015 and 2021 versions of the Russian *Strategy of National Security*. Similar to the 2015 version, it emphasizes the importance of "neutralizing the information impact intended to erode Russia's traditional moral and spiritual values."[227] Just like the 2021 version, the *Doctrine of Information Security* calls for eliminating Russia's dependence on foreign-made IT and InfoSec means by "creating, developing and widely implementing Russian solutions, as well as producing goods and providing services based on such solutions."[228] Similarly, the *Doctrine* proposes developing a national system for managing the Russian segment of the internet.[229]

Both the 2013 and 2016 versions of Russia's *Foreign Policy Concepts* call for promoting the Russian language in the global arena, disseminating information on the achievements of the Russian people, and consolidating the Russian diaspora abroad.[230] Both documents also call for leveraging the capabilities of new ICTs to develop "effective means of information influence on public opinion abroad, strengthen the role

[226] *Strategy of National Security (2021)…* Article IV, Section 57, Clauses 2), 5), 12), 13).
[227] *Doctrine of Information Security…* Article IV, Section 23, Clause j).
[228] *Doctrine of Information Security…* Article IV, Section 25, Clause b).
[229] *Doctrine of Information Security…* Article IV, Section 29, Clause e).
[230] *Foreign Policy Concept (2013)…* Article I, Section 4, Clause h); *Foreign Policy Concept (2016)…* Article III, Section 45, Clause e).

of Russian mass media in the international information environment [and] providing them with essential state support."[231]

4. Proposed Foreign Policy Actions

Russia's proposed foreign policies pertaining to InfoSec largely revolve around its continued efforts to advocate a more international system of internet governance. Moscow wants to establish a legal framework for an IIS system that would help preserve strategic stability. Russia's doctrinal documents consistently emphasize the need for regional cooperation and the promotion of international law regulating military activities in cyberspace via a UN security treaty.

For example, Russia's 2011 *Armed Forces' Information Space Activities Concept* states that the Russian government will "strive for concluding an international cyberspace security treaty under the auspices of UN" to extend principles of international law to cyberspace.[232] The document also expresses hope that Russia will establish InfoSec cooperation with member states of the Collective Security Treaty Organization (CSTO), the Commonwealth of Independent States (CIS), and the Shanghai Cooperation Organization (SCO). Russia's *Military Doctrine* of 2014 also contains calls for developing an international dialogue. The latter should focus on national approaches to addressing military risks and threats stemming from the use of ICTs, according to the 2014 document.[233]

[231] *Foreign Policy Concept (2013)…* Article III, Section 41; *Foreign Policy Concept (2016)…* Article III, Section 47.
[232] *Information Space Activities Concept…* Section 3.1.
[233] *Military Doctrine…* Article III, Section 55, Clause f).

In its 2015 *Strategy of National Security*, the Russian government states its intention to contribute to the development of the IIS system to help preserve strategic stability.[234] In the updated 2021 draft, Russia expands its list of foreign policy goals, adding the need to establish an international legal regime of security in the use of ICTs, bring "reliable information" about Russia's domestic and foreign policies to the Russian and international public, and strengthening the presence of the Russian media in the global information space.[235]

The Russian *Doctrine of Information Security* of 2016 sets similar goals by proposing the establishment of a legal framework for an IIS system and promoting in international organizations Russia's view of equitable cooperation in the information sphere.[236] Similarly, both Russia's 2013 and 2016 *Foreign Policy Concepts* state the government's intention to create under the UN auspices, universal rules of responsible behavior in cyberspace and make the current internet governance regime more international in nature.[237]

5. The Ends, Ways, and Means of Russia's Stated Information Security Strategy

While Russia's posture in the information domain sometimes shifts between defensive and assertive, overall, the Kremlin is notably consistent in its doctrinal statements pertaining to information security. The recurring themes outlined above form a distinctive throughline across all the reviewed doctrines. By examining these themes through the lens of strategic theory, I can now uncover the value system of the Russian

[234] *Strategy of National Security (2015)…* Article IV, Section 104.
[235] *Strategy of National Security (2021)…* Article IV, Section 57, Clauses 14), 15); Section 101, Clause 2).
[236] *Doctrine of Information Security…* Article IV, Section 29, Clause d).
[237] *Foreign Policy Concept (2016)…* Article III, Section 28.

State, how it perceives the strategic InfoSec environment, and how these elements guide the Kremlin's pursuit of its interests.

Table 1 below constitutes my summary of how Russia's aforementioned doctrinal documents described InfoSec threats to the country and opportunities to defend or advance Russia's InfoSec interests in the research period. The table also summarizes what actions these documents prescribed to defend or advance Russia's InfoSec interests. In doing so, Table 1 follows the postulate of strategic theory, which assumes that political actors have interests and will make rational decisions to pursue those interests.

Table 1. Summary of perceived InfoSec threats, opportunities to defend or advance InfoSec interests, proposed domestic and foreign policy actions pertaining to InfoSec as outlined in Russia's main security doctrines from 2011-2021.

Document	Perceived InfoSec Threats	Opportunities to Defend or Advance InfoSec Interests	Proposed Domestic Policy Actions	Proposed Foreign Policy Actions
Armed Forces' Information Space Activities Concept (2011)	States developing their own offensive IW concepts in order to disrupt and gain access to the information spheres of other states.	Utilizing cyberspace to strengthen Russia's defensive capacity; leveraging Russia's scientific and production potential to create advanced cyberspace technologies and skilled personnel.	Developing an InfoSec system for the Armed Forces that would enable early detection, prevention, and settlement of cyberspace military conflicts; using the Russian military colleges to train new information space specialists.	Concluding an international cyberspace security treaty under the auspices of the UN; establishing InfoSec cooperation with member states of the CSTO, CIS, and SCO.
Military doctrine (2014)	The use of ITs to undermine Russia's sovereignty, and political and regional stability; subversive domestic information activities aimed at undermining historical, spiritual, and patriotic traditions.	Utilizing modern ITs to "assess and forecast the development of the military and political situation at global and regional levels, as well as the state of interstate relations in the military-political field." Using non-military means to neutralize potential military risks and threats.	Enhancing capacity and means of IW; creating conditions that would reduce the risk of using ICTs for military-political purposes.	Developing an international dialogue on national approaches to addressing military risks and threats stemming from the use of ICTs.
Strategy of National Security (2015)	The use of ITs by other states to manipulate public opinion and falsify Russian history; external cultural and	Developing informational measures to ensure strategic deterrence and prevent the use of armed force against Russia; taking measures to protect the Russian citizens	Establishing better government control in the information sphere; creating state-funded internet resources, movies,	Contribute to the development of the IIS system to help preserve strategic stability.

	information expansion, including Western pop culture, and the decline in the role of the Russian language in the world.	from the destructive influence of foreign propaganda; making Russia more technologically independent from the West in the information sphere.	print media, television and radio programs, as well as a common “information-telecommunications medium on the territories of the CIS member states and in contiguous regions.”	
Strategy of National Security (2021)	Information space being used as a new sphere of warfare; information campaigns carried out to form a hostile image of Russia; restricted use of the Russian language and the banning of Russian media; increased vulnerability of Russian information infrastructure due to the use of foreign ITs.	Developing a safe information space; protecting the Russian society from destructive information and psychological impacts; developing and implementing information measures aimed at preventing the use of military force against Russia and protecting its sovereignty and territorial integrity.	Developing a system for forecasting, identifying, and preventing InfoSec threats; increasing security, resilience, and freedom from foreign control of the Russian internet and other ICT infrastructure; using Russian-made ITs, as well as advanced technologies, such as artificial intelligence and quantum computing.	Establishing an international legal regime of security in the use of ICTs, bringing “reliable information” about Russia’s domestic and foreign policies to the Russian and international public; strengthening the presence of the Russian media in the global information space.
Doctrine of Information Security (2016)	Growing number of computer crimes, “blatant discrimination” of the Russian media abroad, biased assessments of Russian policy by foreign media, and external information pressure that aims to erode Russian traditional spiritual and moral values.	Countering foreign influence in the information sphere and suppressing activity in cyberspace that is detrimental to national security; leveraging IT to support the Russian culture and provide both the Russian and international communities with the Kremlin’s official point of view on world events; supporting the development and production of competitive InfoSec products and services.	Creating, developing, and implementing Russian IT and InfoSec solutions, as well as producing goods and providing services based on such solutions; developing a national system of Russian internet segment management.	Establishing a legal framework for an IIS system; promoting in international organizations Russia’s view of equitable cooperation in the information sphere.
Foreign Policy Concept (2013)	The use of ITs for international terrorism and criminal activities; unlawful use of soft power, which includes information methods and technologies, to exert political pressure on sovereign states.	Providing the world with accurate information about Russia’s point of view on major international issues, Russian foreign policy initiatives, government actions, and achievements of Russian culture and science.	Providing governmental support to Russian-language media operating in the global information space; developing effective means of information influence on public opinion abroad.	Developing, under the UN auspices, an international code of conduct for InfoSec; advocating more international internet governance.
Foreign Policy Concept (2016)	The use of ITs for international terrorism and criminal activities; information pressure exerted on Russia by	Bolstering the Russian media and communication tools in the global information space and conveying Russia’s perspective on key international issues, Russian	Developing effective ways to influence foreign audiences; promoting the Russian language and Russian-language media in the global	Developing, under the UN auspices, universal rules of responsible behavior with respect to international

	the U.S. and its allies.	foreign policy initiatives, and cultural and research achievements to a wider international community.	information space and providing them with necessary government support.	cybersecurity, including by rendering the internet governance more international in a fair manner.

By analyzing descriptions of these threats, interests, and proposed actions as described in these documents, I was able to infer the following propositions about what constituted Russia's stated information security strategy in the research period, including:

1. Its goals (*ends*) in the form of protecting Russia's citizens, society, and the State from specific internal and external information threats.
2. The legal-administrative, political, economic, social-psychological, and military measures (*means)*, that this strategy prescribed for the purpose of attaining these goals.
3. How (in what *ways*) these *means* were supposed to be employed in order to attain these *ends*.

In particular, I inferred that the goals (*ends)* of Russia's stated InfoSec strategy included defending against the following threats: use of ITs to undermine Russia's sovereignty, political and regional stability; discrimination of the Russian language and media abroad; biased assessments of Russian policy; Russia's dependence on foreign IT; as well as subversive information activities aimed at undermining traditional moral, spiritual, and patriotic values.

I have also inferred that, in order to attain the aforementioned *ends*, Russia's stated InfoSec strategy called for the employment of various legal-administrative, political, economic, social-psychological, and military measures (*means)* in six distinct *ways* that included: (1) leveraging ITs to strengthen the capabilities of the Russian military and InfoSec services; (2) developing domestic IT sectors; (3) utilizing the spheres of culture and education; (4) growing the Russian soft power through the promotion of the Russian media in the global information space; (5) controlling the domestic information environment; and (6) shaping and defining norms of InfoSec and global internet governance via international treaties.

To advance this stated InfoSec strategy, the Russian doctrines proposed a number of specific domestic and foreign policy actions that I summarized in Table 1. Strategic theory tells us that the Russian government would use the aforementioned elements of its stated InfoSec strategy to create more favorable outcomes by choosing how (in what *ways*) it would use the available resources (*means*) in order to accomplish the goals (*ends*) outlined by its policy. However, one should keep in mind that the <u>stated</u> *ends, ways*, and *means* of a strategy do not always align with the actual behavior. Therefore, to understand whether Russia indeed followed its stated strategy, I have inferred thirteen testable propositions regarding the Russian State's expected behavior from domestic and foreign policy actions that the aforementioned strategic documents proposed in the InfoSec domain. These are as follows:

A. To pursue its strategic goal of defending the State against the perceived information threats, the Russian government would work on enhancing its capacity and means of IW.

B. To the same end, the Russian government would launch efforts to train new information space specialists.

C. To further enhance its InfoSec capabilities, the Russian government would use the means of its military to develop an IT-based system for assessing and forecasting the military and political situations at global and regional levels.

D. To increase its own information security, the Russian government would use its legal-administrative and/or economic means to become less dependent on Western ITs.

E. The Russian government would use the available economic means to invest in the scientific and high-tech industries with the goal of creating advanced IT and InfoSec solutions, goods, and services for domestic and international markets.

F. To defend against the perceived threat of the subversive foreign information influence and discrimination of the Russian language abroad, the Russian government would promote traditional moral, spiritual, and patriotic values among its citizens, as well as the study of the Russian language abroad by using the social-psychological means of culture and education.

G. To further defend against foreign information influence, the discrimination of the Russian media, and biased assessments of Russian policy abroad, the Russian government would employ its economic means to create state-funded media and information resources that would provide both domestic and international audiences with the Kremlin's point of view on Russian policies and world events.

H. The Russian government would also work on developing its own effective means of information influence on public opinion abroad.

I. To prevent the use of ITs to undermine Russia's sovereignty, political and regional stability, the Kremlin would use available legal-administrative means to establish better government control within its information sphere.

J. The Russian government would take further legal-administrative measures to protect Russian citizens from perceived foreign information influence.

K. To protect Russia's information space sovereignty, the government would work on developing a national system of Russian internet segment management.

L. Russia would use the political means of diplomacy to advance its InfoSec interests by increasing cooperation on InfoSec issues with member states of the CSTO, CIS, and SCO.

M. To the same end, the Russian government would employ similar means to conclude an IIS treaty under the auspices of the UN and continue to advocate more international internet governance.

This chapter reviewed and analyzed key statements pertaining to InfoSec made in Russia's strategic doctrines issued in 2011-2021. It identified key themes that are consistently reiterated throughout the examined documents. These themes pertain to Russia's perceived InfoSec threats, opportunities to defend or advance InfoSec interests, as well as proposed domestic and foreign policy actions. Based on the identified themes, I was able to construct a broad outline of Russia's stated InfoSec strategy, which can be described as focusing on "shielding" its citizens, society, and the State, from internal and external information threats, including the use of ITs to undermine Russia's sovereignty, political and regional stability; discrimination of the Russian language and media abroad; biased assessments of Russian policy; Russia's dependence on foreign ITs; as well as subversive information activities aimed at undermining traditional moral, spiritual, and patriotic values.

In particular, I established that this stated strategy's three components (*ends, means*, and *ways*) are as follows: (1) attaining protective *ends*, such as securing against the stated information threats; (2) utilizing legal-administrative, political, economic, social-psychological, and military *means* to achieve those *ends*; and (3) employing six distinct *ways* to implement those *means*. The *ways* included leveraging ITs to strengthen the capabilities of the Russian military and InfoSec services; developing domestic IT sectors; utilizing the spheres of culture and education; growing the Russian soft power by promoting the Russian media; controlling the domestic information environment; and shaping and defining norms of InfoSec and global internet governance via international treaties. I have also inferred testable propositions regarding the Russian State's expected behavior and resource allocation decisions. The following chapter will examine Russia's observable behavior and resource allocations in the InfoSec domain in 2011-2021 to ascertain whether these propositions are valid.

Chapter III.

Actions: Russia’s Information Security Strategy in Practice

Whereas Chapter II focused on analyzing Russia's *words* pertaining to its InfoSec strategy, this chapter will examine the government's *actions*. In the previous chapter, I advanced thirteen propositions regarding Russia’s expected behavior that are rooted in the stated *ends, means,* and *ways* of its stated InfoSec strategy. Now, I will test these propositions by correlating them with observable actions by the Russian government during my 2011-2011 research period.

Building on the findings of the scholars reviewed in Chapter I of this thesis, I will examine the activity of the Russian State and its primary agents involved in Russia’s InfoSec and IW operations to explore what, if any, cognitive warfare tactics the government employed to influence public opinion abroad; and analyze how the Kremlin addressed its InfoSec concerns by regulating the Russian segment of the internet. I will also inspect how the Russian government used the social-psychological means of culture, education, and mass media to pursue its strategic ends, and review Moscow’s attempts to shape and define the norms of international information security. In order to assess how well Russia’s stated InfoSec strategy was reflected in its domestic and foreign policy actions, I will examine data from Russia’s federal budget, review key IW capability improvements, and assess whether the Russian government has implemented any structural changes to its cybersecurity forces, introduced new legislation, policies, or made strategic investments in the information technology sector.

If the Russian government’s actions indeed followed its stated InfoSec strategy, then I should be able to find robust evidence that its actions and resource allocations corresponded with the behavior my propositions anticipated. If, however, the Russian state's actions contradicted the anticipated behavior, then the evidence, which I would find, will indicate that there was no alignment between words and actions when it comes to Russia's InfoSec strategy.

A. Enhancing Russia's Capacity and Means of Information Warfare

My proposition "A" is that, to pursue its strategic end of defending itself against the perceived information threats, the Russian State would work on enhancing its capacity and means of IW. To test this proposition, the following section will examine whether the Russian authorities took significant steps to attain that goal in the 2011-2021 period. I will begin by providing a broad overview of key actors involved in Russia's InfoSec and IW activities. Since electronic warfare (EW) is an important subset of IW, I will also examine the expansion of the role of EW in the Russian Armed Forces.

1. Primary Actors Involved in Russia's Information Security and Information Warfare Operations

The Russian government is notoriously cagey about the organizations and agencies involved in information operations, so very little open-source information is available on this subject. My analysis of publicly available documents, academic literature, and news reports indicates that Russia's IW efforts are mainly conducted through three parallel structures: the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU). The latter acts as the Russian military intelligence service and is more commonly known by its Soviet abbreviation GRU – the Main Intelligence Directorate.[238]

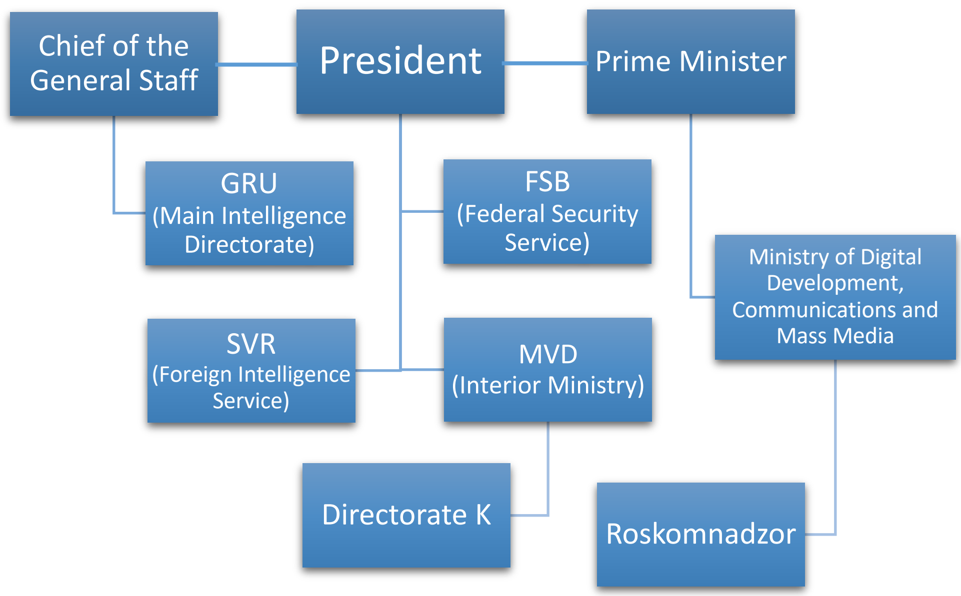

Figure 2. Russia's information security architecture

The FSB is Russia's main domestic security agency responsible for surveillance, counterintelligence, and defense against cyberattacks on government systems and critical infrastructure sites. Favored by Vladimir Putin – who served as the Director of the Federal Security Service prior to becoming President in 1999 – the FSB is also the most politically powerful of the three security and intelligence agencies discussed here.[239] Over

---

[238] Conor Cunningham. "A Russian Federation Information Warfare Primer." The Henry M. Jackson School of International Studies. University of Washington. November 12, 2020. Accessed July 30, 2022. https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/#_ftn11
[239] Mark Galeotti. "Rossiyskaya Razvedka Vedet (Politicheskyu) Voinu [Rusian Intelligence Conducts (Political) War]." *The NATO Review*. May 12, 2017. Accessed July 30, 2022.

the period of his presidency, Putin has continually increased the FSB budget and expanded its reach.[240]

The FSB oversees and operates the System for Operative Investigative Activities (SORM), which is Russia's system for surveilling domestic telephone and internet communications.[241] In 2013, Putin ordered the FSB to create a state system for detecting, preventing and eliminating the consequences of cyberattacks.[242] After several years of development, the FSB unveiled the system known as GosSOPKA (State System for Detecting, Preventing and Eliminating the Consequences of Computer Attacks or Gosudarstvennaya Sistema Obnaruzheniya, Preduprezhdeniya I Likvidatsii Posledstviy Kompyuternykh Atak). The system works via several response centers that constantly monitor government information resources and critical infrastructure sites and share information about any cyberattacks with the FSB's National Coordination Center for Computer Incidents (Gov-CERT).[243] The Center then analyzes the incidents and provides prevention and response recommendations to the rest of the system. In 2016, the head of Gov-CERT Alexey Novikov reported that GosSOPKA's response centers were set up at Russia's Central Bank and state-owned defense conglomerate Rostec, and that the system had already extended to ten government agencies.[244]

https://www.nato.int/docu/review/ru/articles/2017/05/12/rossijskaya-razvedka-vedet-politicheskuyu-vojnu/index.html

[240] Galeotti, "Rusian Intelligence Conducts…"

[241] Andrei Soldatov and Irina Borogan. "The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries." *Public Affairs*, 2015.

[242] Sasha Baranovskaya. "Moscow's cyber-defense: How the Russian government plans to protect the country from the coming cyberwar." *Meduza*. July 19, 2017. Accessed July 30, 2022. https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense

[243] Baranovskaya, "Moscow's cyber-defense…"

[244] Veniamin Petrov. "'Rosteh' zanyalsya parirovaniem kiberugroz ['Rosteh' engaged in parrying cyber threats]." *Izvestiya.* November 7, 2016. Accessed July 30, 2022. https://iz.ru/news/642771

The two main cyber departments within the FSB, however, are the 16th and 18th Centers for Information Security (ISC).[245] Initially tasked with defending Russia's internet from hackers, the ISCs have in recent years expanded their operations beyond state borders.[246] In 2017, the U.S. government indicted Russian FSB officers from the 18th Center for hacking Yahoo and millions of email accounts.[247] The ISCs also reportedly focus on targeting foreign infrastructure and the energy sector for both reconnaissance and offensive operations.[248] They are known to have close connections with private companies, criminal and civilian hackers, as well as government scientific research centers, which they use to augment their staff and cyber operations.[249] Some of these scientific research centers include Moscow-based "Kvant," "Voskhod," and the "Atlas" Scientific and Technical Center. The centers are engaged in the development and testing of new cyber-defense systems, as well as certification of foreign software before it can be used by state agencies.[250] In December 2017, the Russian government nationalized "Atlas" by turning it into a joint-stock company where 100 percent of the stock is owned

---

245 Andrew S. Bowen. "Russian Cyber Units." Congressional Research Service. IF11718, Version 4. Updated February 2, 2022. Accessed July 30, 2022. https://crsreports.congress.gov/product/details?prodcode=IF11718

246 Andrei Soldatov and Irina Borogan, "Russia's Approach to Cyber: The Best Defence is a Good Offence." European Union Institute for Security Studies (EUISS). 2018. Accessed July 30, 2022. https://www.jstor.org/stable/resrep21140.5

247 "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts." The United States Department of Justice. Press release. March 15, 2017. Accessed July 30, 2022. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

248 Bowen, "Russian Cyber Units."

249 Pavel Luzin. "Rossiyskie kibervoiska: celi i protivorechiya [Russian cyber troops: goals and contraditions]." *Riddle.io*. April 28, 2021. Accessed July 30, 2022. https://ridl.io/rossijskie-kibervojska-celi-i-protivorechija/

250 Baranovskaya, "Moscow's cyber-defense…"

by the State.[251] As of 2020, this center was reported to have 1,600 government contracts totaling 13.9 billion rubles (or $193,2 million in 2020 equivalent).

Russia's Foreign Intelligence Service (SVR) is responsible for collecting intelligence abroad using human, signals, and cyber methods. The agency possesses a high level of internal cyberspace capabilities and has targeted multiple critical infrastructure organizations since at least 2008.[252] The SVR's primary targets include government networks, think tanks, and information technology companies.

For instance, the SVR-affiliated hacking group, known as COZY BEAR[253] along with the GRU-affiliated group, known as FANCY BEAR, was allegedly implicated in the hacking of the Democratic National Committee email servers in 2015-2016, ahead of the U.S. presidential election.[254] On April 15, 2021, the White House accused the SVR of the 2020 hacking of the Orion software produced by Texas-based company SolarWinds.[255] The attack compromised an entire global technology supply chain that affected hundreds of private companies, U.S. government agencies, and critical infrastructure facilities. That same year, the SVR also allegedly targeted British, Canadian, and American

---

[251] "Byvshuu IB-kompaniu FSB prevratili v akcionernoe obwestvo [Former FSB cybersecurity company was turned into a joint-stock company]." *C-News*. September 22, 2020. Accessed July 30, 2022. https://www.cnews.ru/news/top/2020-09-22_byvshuyu_ibkompaniyu_fsbotdannuyu

[252] Alert (AA22-110A) "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." The U.S. Cybersecurity & Infrastructure Security Agency. April 20, 2022. Last revised: May 9, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[253] Also known as APT29 and The Dukes.

[254] "CrowdStrike's work with the Democratic National Committee: Setting the record straight." Crowdstrike. June 5, 2020. Accessed July 30, 2022. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

[255] "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government." The White House. April 15, 2021. Accessed February 5, 2023. https://bit.ly/3IdqskP

organizations with the goal of stealing research data on the development of the coronavirus vaccine to speed up Russia's own vaccine development.[256]

Like the FSB, the SVR works with private IT companies and government research centers, like AO Pasit and Federal State Autonomous Scientific Establishment "Scientific Research Institute for Specialized Security Computing Devices and Automation" (SVA). Both entities conduct research and development supporting the SVR's malicious cyber operations.[257] However, while Western cybersecurity experts have attributed cyberattacks to the SVR for many years, little is known about the chain of command inside the agency or particular units responsible for these activities.

The GRU is also tasked with gathering foreign intelligence. However, unlike the FSB and the SVR, it is part of the Russian Armed Forces. The GRU cyber departments consist of three primary units. Units 26165 and 74455 are focused on conducting cyberattacks in almost every part of the world, while Unit 54777 (also known as 72nd Special Service Center) is thought to be responsible for information-psychological operations, such as online disinformation campaigns.[258] While the FSB and the SVR use the help of private actors, as well as government scientific research centers to support their operations, the GRU leans primarily on military-scientific organizations, such as the 27th Central Research Institute, Technopolis "ERA," and special scientific companies – military units comprised of science and engineering students.[259]

---

256 Julian E. Barnes. "Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say." *The New York Times*. Published July 16, 2020, updated December 14, 2020. Accessed February 5, 2023. https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html
257 "Treasury Sanctions Russia with Sweeping New Sanctions Authority." U.S. Department of the Treasury. April 15, 2021. Accessed February 5, 2023. https://home.treasury.gov/news/press-releases/jy0127
258 Bowen, "Russian Cyber Units."
259 Luzin. "Russian cyber troops…"

The GRU appears to be the most active of the three agencies when it comes to conducting cyberattacks. It has been implicated in some of the most damaging attacks, including the 2014 Sandworm and 2017 NotPetya malware used against Ukraine.[260] The GRU was also one of the two Russian intelligence agencies, along with the SVR, accused of hacking the Democratic National Committee. While the SVR's COZY BEAR was the first to breach the committee's computers in 2015, investigators believe the GRU played a bigger role in releasing the stolen emails.[261] As a result, in July of 2018, the U.S. Department of Justice announced an indictment charging twelve Russian nationals – all of whom were members of the GRU – with federal crimes for interfering with the 2016 U.S. presidential election.[262]

Interestingly enough, both agencies seem to have conducted their cyberattacks independently from one another. According to cybersecurity firm CrowdStrike which investigated the breach, there was no collaboration between COZY BEAR and FANCY BEAR, and both groups compromised the same systems and stole identical information at different points in time.[263] Such behavior, however, is not uncommon for Russian intelligence agencies. Despite the broad range of actors involved in Russian cyber operations, Moscow doesn't have a unified cyber command. In fact, according to Mark Galeotti, an expert on Russian security issues, Russia's main intelligence agencies coexist

---

[260] Keir Giles and Valeriy Akimenko. "Russia's Cyber and Information Warfare." *Asia Policy*. 2020. Roundtable: The Future of Cybersecurity across the Asia-Pacific. Accessed July 30, 2022. https://www.academia.edu/42893415/Russia_s_Cyber_and_Information_Warfare?auto=citations&from=cover_page

[261] "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election." Department of Justice Office of Public Affairs. Press Release. July 13, 2018. Accessed February 5, 2023. https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

[262] See "Grand Jury Indicts…"

[263] See "CrowdStrike's work with the Democratic National Committee…"

in a highly adversarial relationship with one another.[264] They often engage in parallel cyberattacks, replicating each other's work, stealing sources, and even compromising each other's operations, according to Galeotti.

In addition to the three agencies discussed above, the Russian Interior Ministry's Directorate K focuses primarily on investigating IT-related crimes, such as the creation, use, and distribution of malicious programs, IT-related fraud, copyright violations, and the production and distribution of pornographic content directed against minors. According to an archived page from its website, the Directorate is also responsible for combating international cybercrimes and cooperates with its counterparts in foreign states.[265] Directorate K is one of the most secret divisions of the Interior Ministry.

Finally, another important element of Russia's information warfare machine is Roskomnadzor or the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies, and Mass Communications. When it was created in 2008, the regulatory agency had only a dozen employees tasked with overseeing radio signals, telecommunications, and the Russian mail service. However, as the Kremlin's InfoSec concerns grew following the Arab Spring of the 2010s and the 2011 anti-government protests in Moscow, Vladimir Putin began to transform Roskomnadzor into a powerful surveillance and censorship apparatus, vastly expanding its authority and tasking it with overseeing the internet.[266]

---

[264] Mark Galeotti. "Putin's Hydra: Inside Russia's Intelligence Services." European Council on Foreign Relations. Policy Brief. May 2016. Accessed July 30, 2022. https://bit.ly/41ak9Y4

[265] "Upravlenie 'K' MVD Rossii [Directorate 'K' MVD Russia]." Interior Ministry of the Russian Federation. Archived June 14, 2015. Accessed via the Wayback Machine February 14, 2023. https://bit.ly/3Z7rQMR

[266] Paul Mozur et al. "'They Are Watching': Inside Russia's Vast Surveillance State." *The New York Times.* September 22, 2022. Accessed February 15, 2023. https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html

Starting in 2012, when Putin retook the presidency, Roskomnadzor began to closely monitor the Russian information sphere, including websites, social media, as well as print, radio, and TV news outlets, often banning websites that criticized the current regime.[267] The agency imposed fines and penalties on tech giants like Google, Twitter, Facebook, and Telegram, forcing them to remove content that authorities deemed illegal. Often cooperating with the FSB, Roskomnadzor also helped identify individuals behind anti-government social media accounts, providing security agencies with detailed information about online critics.

In sum, while most of the organizations and agencies involved in Russia's InfoSec and IW operations demonstrated enhanced capacity for such activities within my 2011-2021 research period, Roskomnadzor appears to have undergone the greatest transformation. The agency grew from an inconspicuous regulatory body into Russia's chief censorship machine with vast resources, political power, and technical capabilities. Together, the organizations and agencies described in this section are responsible for conducting the majority of Russia's foreign and domestic information-technical and information-psychological operations.

2. Expanding Role of Electronic Warfare in Russian Armed Forces

As a subset of the broader concept of IW, electronic warfare (EW) typically refers to a set of activities aimed at intercepting, disrupting, or jamming signals through the use of the electromagnetic spectrum. Russia's *Military Doctrine* of 2014 states the government's focus on enhancing the Armed Forces' capacity and means of IW and

---

[267] Mozur et al. "'They Are Watching…'"

creating conditions that would reduce the risk of using ITs for military-political purposes.[268] Enhancing its EW capabilities enables Russia to increase the information security of its Armed Forces and critical infrastructure by improving their command and control functions, enabling the protection of friendly information systems, as well as interrupting enemy communications. Along with IW, EW also provides Russia with an opportunity to bridge the gap in conventional warfare capabilities with the West.

Russia's strategic focus on EW has been reflected in the government's resource allocations and expansion of the role of EW within the Russian military. Electronic warfare began to play a more prominent role in the Russian Armed Forces in 2009 when the government distinguished EW troops into a separate branch of its military.[269] Since 2011, however, the Kremlin has procured a large number of new EW systems and made EW troops an integral part of Russia's military operations.[270] The Russian 2020 State Armament Program, the GPV (Gosudarstvennaya programma vooruzheniya), which specified the volume of supplied armaments for the period between 2011-2020, designated significant funds for upgrading the military's radio-electronic equipment. Among the program's designated priorities was bringing the Russian EW troops to a 70-percent level of technical modernity by the end of 2020.[271]

"The majority of Russia's future EW specialists study at the 5th faculty for EW and information support of the Air Force Academy in Voronezh.[272] The academy reportedly has advanced EW equipment and training simulators that teach officers tactics

---

[268] *Military Doctrine…* Article III, Section 46, Clause c).
[269] Jonas Kjellen. "Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces." The Ministry of Defense of Sweden. Report no FOI-R-4625-SE. September 2018.
[270] Giles, "Assessing Russia's…"
[271] Kjellen. "Russian Electronic Warfare…"
[272] Kjellen, "Russian Electronic Warfare…"

of IW, EW, and technical reconnaissance. The academy also features an on-site EW scientific research center that works in coordination with the faculty to develop new EW equipment.

The overall number of soldiers serving in the Russian EW units is relatively small. In 2014, approximately 2,700 conscripts were trained at the 1084th training center in Tambov, Russia's main training facility for EW specialists.[273] In 2017, that number decreased to 2,000 conscripts. The reduction in conscripts can be explained by the Ministry of Defense's efforts to increase the number of contract soldiers in its EW units.[274] Overall, research indicates that the number of professional contract soldiers within the Russian Armed Forces has exceeded the number of conscripts, which reflects Russia's stated focus on creating a better-trained and equipped military.[275]

Once EW troops were officially distinguished as a separate branch of the Russian military in 2009, the Kremlin launched an extensive rearmament program to upgrade Russia's EW capabilities. This included the development and production of new command and control and electronic reconnaissance systems, as well as systems capable of jamming aircraft communication, satellite navigation, and suppressing reconnaissance satellites.[276] Some of these new capabilities were put on display during Russian military operations in Ukraine and Syria where it targeted opposing military formations and used jamming equipment to suppress military and civilian communications. This extensive

[273] Kjellen, "Russian Electronic Warfare…"
[274] Kjellen, "Russian Electronic Warfare…"
[275] Giles, "Assessing Russia's..."
[276] Kjellen, "Russian Electronic Warfare…"

application of EW led many military analysts to conclude that Russia has significantly increased its EW capabilities in recent years.[277]

B. Training New Information Space Specialists

It follows from my proposition "B" that, as part of its InfoSec strategy, the Russian government would launch efforts to train new information space specialists. The following section tests this proposition by reviewing the various measures that were implemented in 2011-2021 to establish an IT talent pipeline for organizations within Russia's military-industrial complex.

Poorly funded throughout the 1990s and with antiquated equipment, the Russian military was initially slow to embrace the information sphere.[278] As such, for many years, this domain was exclusive to Russia's intelligence agencies. However, things began to change in the years following the 2011 release of the *Conceptual Views on the Activity of the Armed Forces in the Information Space.* The main threat emphasized by *the Concept* was that foreign states were actively developing offensive IW concepts in order to disrupt and gain access to the information spheres of other states. As one of the ways of addressing this perceived threat, *the Concept* proposed training new information space specialists within the Armed Forces.

As part of Russia's "Education Development" program for 2013-2020, the Kremlin aimed at establishing a talent pipeline for organizations within Russia's military-industrial complex.[279] Within this pipeline, the government planned to provide in-depth

---

[277] Kjellen, "Russian Electronic Warfare…"
[278] Soldatov and Borogan. "Russia's Approach to Cyber…"
[279] Postanovlenie Pravitelstva RF ot 15 aprelya 2014 g. N 295 "Ob utverzhdenii gosudarstvennoy programmy Rossiyskoy Federacii 'Razvitie obrazovaniya' na 2013-2020 gody [Decree of the Government

training for 9,000 specialists who would have signed agreements with organizations of the military-industrial complex. The training would be provided via vocational and higher education programs, as well as through 3,500 online educational courses that were to be created under the same target program.[280]

Additionally, in March 2013, Russia's Defense Minister Sergey Shoigu announced plans for the creation of scientific companies that would be comprised of talented university students.[281] Rather than performing their mandatory military service after graduating, serving within a scientific company would allow students to remain at the university while conducting research that supports the goals of the Russian military. The first recruits were sourced from the Bauman Moscow State Technical University in July of the same year.[282] Besides conducting research, recruits were involved in the development and testing of code for special software, including mathematical and computer modeling.[283]

Also in 2013, Russia's Ministry of Defense announced that it would create a separate branch of the military to combat information threats. Modeled after the U.S. Cyber Command, Russia's information operations troops would include a variety of specialists tasked with the monitoring and processing of information, combating cyber

---

of the Russian Federation of April 15, 2014, N 295 "On Approval of the State Program of the Russian Federation 'Education Development' for 2013-2020"]." Government of the Russian Federation. p.9. Accessed July 31, 2022. https://base.garant.ru/70643472/

280 Decree N 295, pp. 14-15.

281 "Shoigu: Minoborony mozhet nachat' sozdavat' nauchnye roty v universitetah [Shoigu: Ministry of Defense may begin creating scientific companies at universities]." *RIA Novosti* [*RIA News*]. March 12, 2013. Accessed July 30, 2022. https://ria.ru/20130312/926805518.html

282 "Pervye nauchnye roty otpravilis' na sluzhbu [The first scientific companies went to serve]." *Lenta.ru*. July 9, 2013. Accessed February 5, 2023. https://lenta.ru/news/2013/07/09/companies/

283 "Prohozhdenie voennoi sluzhby v nauchnyh rotah [Military service in scientific companies]." Nacional'nyi Issledovatel'skiy Universitet "MEI" [National Research University "MEI"] March 11, 2022. Accessed July 30, 2022. https://mpei.ru/Structure/Universe/mei/Pages/company.aspx

threats, as well as conducting disinformation and counterpropaganda activities.[284] According to some sources, the federal government allocated $70 million to this unit in 2013.[285] Yet other sources note that the Russian equivalent of the U.S. Cyber Command may have been established as early as 2012.[286]

Little was known about the status of this project, and the Russian Parliament had continuously denied its existence.[287] However, in February 2017, Shoigu admitted that the formation of the Russian information operations troops was indeed completed.[288] According to the defense minister, the cyber troops are "much more effective and powerful" than Russia's old counterpropaganda directorate. Shoigu's comparison reinforced the belief that Russia's cyber troops are involved in both information-technical and information-psychological operations.

Later that year, Russian newspaper *Kommersant* cited a study by international cybersecurity firm Zecurion Analytics estimating that Russia's cyber troops numbered approximately 1,000 people and their annual budget may be reaching $300 million.[289] The study placed Russia on the top five list of countries with the most developed cyber

---

[284] "Minoborony mozhet sozdat' otdel'nyi rod voisk po bor'be s kiberugrozami [The Ministry of Defense may create a separate branch of the armed forces to combat cyber threats]." *RIA Novosti* [*RIA News*]. July 5, 2013. Accessed July 30, 2022. https://ria.ru/20130705/947802340.html; also see Giles, "Russia's Cyber and Information Warfare."
[285] Pierluigi Paganini. "Krym: rossiyskaya kiberstrategiya voiny [Krimea: Russian cyber strategy or war]." *Den'* [*Day*]. March 27, 2014. Accessed July 30, 2022. https://day.kyiv.ua/ru/article/ekonomika/krym-rossiyskaya-kiberstrategiya-voyny
[286] A January 2017 edition of Moscow Defense Brief, titled "Russian Information and Cyber Operations," noted that Russia's Defense Ministry established a Cyber Command in 2012.
[287] "V Gosdume oprovergli suwestvovanie "kibervoysk" v Rossii [The State Duma denied the existence of "cyber troops" in Russia]." Interfax. January 16, 2017. Accessed February 12, 2023. https://www.interfax.ru/russia/545640
[288] "V Minoborony RF sozdali voiska informacionnyh operacyi [The Russian Ministry of Defense created the information operations troops]." Interfax. February 22, 2017. Accessed via the Wayback Machine July 30, 2022. https://web.archive.org/web/20220516105752/https://www.interfax.ru/russia/551054
[289] The study itself does not appear in the public domain. For *Kommersant* coverage of the study, see: Maria Kolomychenko. "V internet vveli kibervoiska [Cybertroops have entered the internet]." *Kommersant*. January 10, 2017. Accessed July 30, 2022. https://www.kommersant.ru/doc/3187320

forces, following the U.S., China, the United Kingdom, and South Korea. Former KGB Analysis Directorate Chief Vladimir Rubanov made similar assessments regarding the number of soldiers in Russia's cyber troops.[290] However, little official information has since been released about the structure, size, and capabilities of Russia's new cyber unit.

In 2018, Vladimir Putin signed a decree on the creation of the military technopolis "ERA."[291] Located near the Black Sea resort town of Anapa, the innovation center was meant to operate as a military-civilian partnership where the Russian army elites would work alongside civilians with the support of conscript soldiers serving in the military scientific companies. The project was aimed at strengthening Russia's defense capability by creating an innovative research and development infrastructure.

C. Developing IT-Based System for Assessing and Forecasting Military and Political Situations

My proposition "C" is that to further enhance its InfoSec capabilities, the Russian military would use the means of its military to develop an information technology-based system for assessing and forecasting the military and political situations at global and regional levels. This proposition is based on statements describing the State's intentions to develop such a system that were consistently reiterated throughout several of Russia's strategic doctrines. While researching actions the Russian authorities took in this regard, I found that in 2014, to improve its own command and control capabilities, Russia created

---

[290] Maria Latsinskaya, Aleksandr Braterskiy, and Ignat Kalinin. "Rossiya vvela voiska v internet [Russia Sent Troops onto the Internet]." *Gazeta.ru*, 22 February 2017. Accessed July 30, 2022. https://www.gazeta.ru/tech/2017/02/22_a_10539719.shtml

[291] Mikhail Metcel. "Putin podpisal ukaz o sozdanii voennogo tehnopolisa 'Era' v Anape [Putin signed a decree on the creation of military technopolis 'Era' in Anapa]." TASS. June 25, 2018. Accessed July 30, 2022. https://tass.ru/armiya-i-opk/5322634

the National Defense Management Center.[292] Combining information resources of all ministries and departments under one roof, the center enables the government to collect, summarize, and analyze real-time information coming from the federal executive authorities, primarily those involved in the implementation of the Russian defense plan. Its main function, however, is to coordinate the actions of the Russian Armed Forces and maintain them in a combat-ready state. The center monitors activities across all military units and training grounds and communicates with civilian companies working with the military.[293]

In 2019, Defense Minister Sergey Shoigu declared that the National Defense Management Center has a system capable of predicting outbreaks of armed conflicts and the emergence of hot spots:

> "If we put into the database all the information about actions, for example, formations in Yugoslavia (when, how many ships, with how many carriers, how many planes, how many missiles, at what time - daytime, nighttime, and what was happening at that time), then it's like 'an alarm clock' – it rings and says: 'you know, the situation is very similar in such and such region of the world, because of the same number of ships, aircraft carriers, planes, carriers of cruise missiles, high-precision weapons, so there is a high probability that in this part of the world, the same will occur as what occurred in Yugoslavia.'"[294]

Shoigu noted that the system can also store and systematize information, as well as provide options for potential actions in different scenarios.

---

[292] "Nacionalny centr upravleniya oboronoi Rossii (NCUO RF) [National Defense Management Center of Russia (NDCC RF)]." *TAdviser*. Accessed July 30, 2022. https://bit.ly/3HX8vXw

[293] Igor Lapik. "Serdce rossiyskoi armii: kak rabotaet nacionalny centr upravleniya oboronoi [The Heart of the Russian Army: How the National Defence Center operates]." *Zvezda TV* [*Star TV*]. December 19, 2019. Accessed July 30, 2022. https://tvzvezda.ru/news/201912191737-JcWFf.html

[294] Aleksandr Peshkov. "Shoigu: v MO RF sozdana Sistema prognozirovaniya vooruzhennyh konfliktov [Shoigu: a system for predicting armed conflicts has been created within Russia's Ministry of Defense]." *Zvezda TV* [*Star TV*]. December 16, 2019. Accessed July 30, 2022. https://tvzvezda.ru/news/201912161125-PViRZ.html

D. Lessening Russia's Dependence on Western Information Technologies

In my proposition "D," I posit that, to increase its own information security, the Russian government would use its legal-administrative and/or economic means to become less dependent on Western ITs. To understand whether the government's actions were consistent with this proposition, the following section reviews several federal programs initiated by the Russian authorities between 2011 and 2021. These programs were aimed at promoting domestic IT development, increasing the use of Russian-made software and information-communication technologies across government agencies, and decreasing Russia's dependency on Western IT imports.

In the 2011-2021 period, Moscow allocated trillions of rubles to several federal programs aimed at domestic IT development. On May 5, 2016, the Russian government issued decree No.392 "On priority areas for the use and development of information and communication technologies in federal executive bodies and management bodies of state non-budgetary funds and on amendments to some acts of the Government of the Russian Federation."[295] The decree outlined a government-wide program designed, among other things, to increase the use of Russian-made software and information-communication technologies across government agencies. This, in turn, was meant to decrease Russia's dependency on Western technology while increasing its information security and providing wider access to state information resources for Russian citizens.[296]

[295] Postanovlenie Pravitelstva RF ot 5 May 2016 g. N 392 "O prioritetnyh napravleniyah ispolzovaniya i razvitiya informacionno-kommunikacionnyh tehnologiy v federalnyh organah ispolnitelnoi vlasti i organah upravleniya gosudarstvennymivnebudjetnymi fondami i o vnesenii izmeneniy v nekotorye akty Pravitelstva Rossiyskoy Federacii [Decree of the Government of the Russian Federation of May 5, 2016 N 392 "On priority areas for the use and development of information and communication technologies in federal executive bodies and management bodies of state extra-budgetary funds and on amendments to some acts of the Government of the Russian Federation"]." The Russian Federation. Accessed July 30, 2022. https://base.garant.ru/71394834/#block_12

[296] See Decree N 392 "On priority areas…" Section 3, Clauses е) and ж), as well as Section 8, Clause г).

A year later, the Ministry of Digital Development, Communications, and Mass Media published another approved decree, No.334, which was aimed at transitioning federal executive bodies and state off-budget foundations to the use of domestic office software.[297] The decree mandated all federal departments to adopt strict plans to start using only domestic office software within the 2018-2020 period. In order to purchase new computers with pre-installed Microsoft Windows and Office software, federal departments would need to first provide their justifications for the impossibility of using Russian alternatives and receive explicit approval from the Ministry.

According to government data, the 2016 budget allocated for the digitization of federal government agencies was increased by nearly 10 percent to 117,1 billion rubles (equivalent to approximately $1.75 billion in 2016).[298] This amount continued to increase steadily, and by 2019, Russia's IT spending rose to 140.29 billion rubles ($2.17 billion). However, it should be noted that only about 30 percent of these funds were typically spent on the development of new technologies while the rest was used for the upkeep and maintenance of existing IT infrastructure.[299] In 2020, the government separated IT spending into its own line of expenses within the federal budget for 2021-2023.[300]

---

[297] "Analiz federalnogo budzheta na razvitie informacionnyh tehnologiy: nastoyawee I buduwee [Analysis of the federal budget for the development of information technologies: the present and the future]." Research and production complex "Integral." September 26, 2017. Accessed July 30, 2022. https://integral-russia.ru/2017/09/26/analiz-federalnogo-byudzheta-2017-goda-na-razvitie-informatsionnyh-tehnologij/
[298] Data for 2011-2013 and 2020-2021 was not available. For 2014-2019 data, see Accounts Chamber of the Russian Federation. "Reiting IT-rashodov federalnyh gosorganov [Rating of the Federal Government IT-spending]." Accessed July 30, 2022. https://spending.gov.ru/analytics/ratings/it/
[299] "Internet-trafik RF pod control' [RF internet-traffic under control]." *TAdviser.* Accessed July 30, 2022. https://bit.ly/3S1A5Yn
[300] "Gosudarstvennye infosistemy budut finansirovatsya po otdelnomu kodu rashodov [Government info-systems will be financed according to a separate cost code]." Ministry of Digital Development, Telecommunications and Mass Media of the Russian Federation. July 28, 2020. Accessed July 30, 2022. https://digital.gov.ru/ru/events/39978/

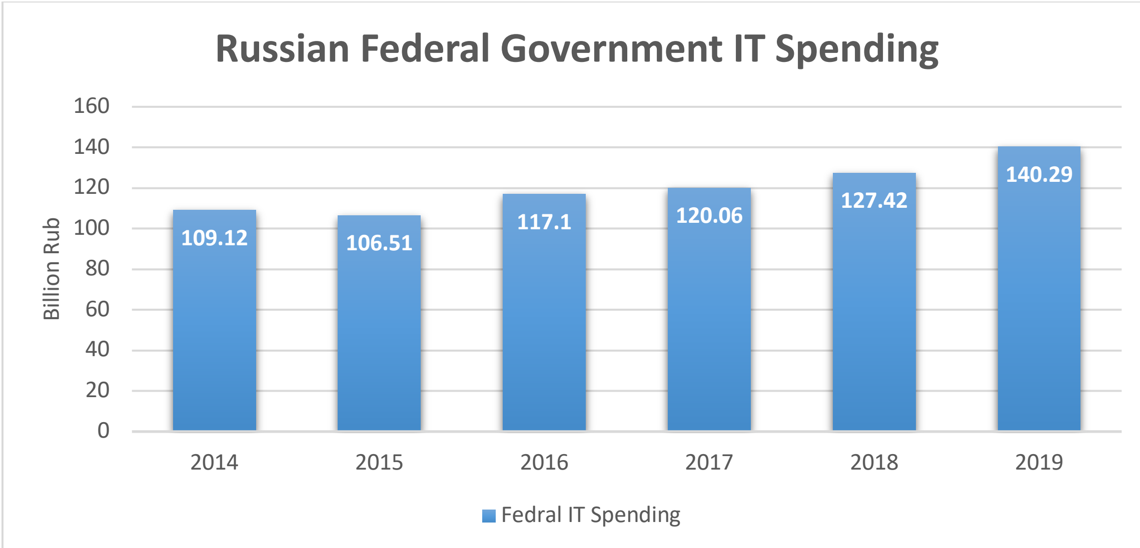

Figure 3. The Russian government's annual information technology budgets 2014-2019

In June 2016, Russia's Ministry of Digital Development, Communications, and Mass Media published decree No.206 approving the plan of its activities for the period 2016-2021.[301] Featuring seventy-nine specific performance targets, the ambitious plan focused on the following eight areas of Russian society:

1. Ensuring the provision of state, municipal, and socially important services to citizens and organizations in electronic form and improving the quality of public administration;
2. Improving the quality of life of citizens with the introduction of the state information system of housing and communal services;
3. Achieving a high pace of development in the information technology industry;

[301] Prikaz N 206 "Ob utverzhdenii plana deyatelnosti Ministerstva svyazi i massovyh kommunikaciy Rossiyskoy Federacii na period 2016-2021 godov [Decree No 206 "On approval of the activity plan of the Ministry of Telecommunications and Mass Media of the Russian Federation for the period of 2016-2021]." The Ministry of Telecommunications and Mass Media of the Russian Federation. May 20, 2016. Accessed July 30, 2022. http://filearchive.cnews.ru/img/cnews/2016/06/29/16062016p24_5458vn.pdf

4. Providing high-quality and modern postal services in the Russian Federation;
5. Ensuring equal access to communication services and the Internet;
6. Ensuring equal access to the media environment;
7. Improving the quality and intensity of information exchange with foreign countries, access to the main information flows (legal, economic, and business information);
8. Providing information support for the fight against terrorism and ensuring public safety.

To strengthen the Russian IT sector, the plan declared that by the end of 2016, the volume of domestic production in the industry should reach 390 billion rubles ($5.85 billion), and by 2021, increase to 700 billion ($10.5 billion). Additionally, the Russian IT industry should generate 15,000 high-performance jobs annually.

To expand Russia's information infrastructure, the plan tasked the Ministry of Telecommunications and Mass Media with increasing broadband internet access from 75 percent of the total number of households in 2016 to almost 100 percent by 2021. Similar goals were set for the proportion of the population with high-definition television reception. The plan also included a number of activities to help support Russian media – another priority of Russia's stated InfoSec strategy. For example, it outlined the provision of support to organizations producing or disseminating "socially important" or "educational" projects in digital media. Up to 165 such projects were to be supported by the government each year.

At the same time, Russia's state-owned international TV network "*Russia Today*" (which has since been renamed to "*RT*") was to increase its total broadcasting time from

106 hours per day in 2016 to 166 hours by 2020. The plan also presented a timeline for the creation of additional TV networks broadcasting in English, Arabic, and Spanish languages. According to the document, by the year 2021, this and other outlined measures were supposed to increase the size of the Russian digital media's foreign audiences by at least 15 percent.

In July 2017, Russia's Prime Minister Dmitry Medvedev approved another federal program titled "The Digital Economy of the Russian Federation." Designed to fully transition the Russian economy into the digital age by 2024, the program aims to organize the systemic development and implementation of digital technologies in all areas of life, including the economy, public administration, and the social sphere. According to Medvedev, the transition of Russia's economy into the digital age is "a matter of our global competitiveness and national security."

The program's main targets include:

1. Increasing government spending on the development of the digital economy by at least 300 percent by 2024;
2. Creating a stable and secure IT infrastructure for transmitting, analyzing, and storing large amounts of data, which would be accessible to most organizations and households;
3. Using predominantly domestic software across state bodies, local authorities, and organizations.[302]

[302] Rasporyazhenie ot 28 iulya 2017 g. No 1632-r: "Utverdidt prilagaemuu programmu 'Cifrovaya Ekonomika Rossiyskoy Federacii' [Order from July 28, 2017, No 1632-r: "Approve the attached program 'Digital Economy of the Russian Federation'"]." Government of the Russian Federation. Accessed July 30, 2022. http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

To accomplish these goals, the program focuses on six areas that include regulation, digital governance, education and training of personnel, as well as the development of scientific and technical capabilities, IT infrastructure, and cybersecurity. It allocates 5 billion rubles (or $83 million in 2017) annually to help generate qualified personnel. This money enables approximately one million Russians each year to access online graduate education programs in the field of the digital economy.

As of 2018, the total budget of the Russian Digital Economy program was 1.64 trillion rubles or about $25 billion.[303] However, in 2019, the Russian government expanded the program to include the development of artificial intelligence (AI) technologies through 2030.[304] The AI program's goal is to turn Russia into one of the world leaders in the field.

[303] See Order from July 28, 2017, No 1632-r…
[304] Ukaz Presidenta RF ot 10 oktyabrya 2019 g. N 490 "O razvitii iskustvennogo intellekta v Rossiyskoy Federacii [Presidential Decree of October 10, 2019, N 490 "On the development of artificial intelligence in the Russian Federation"]." Government of the Russian Federation. Accessed July 30, 2022. https://base.garant.ru/72838946/

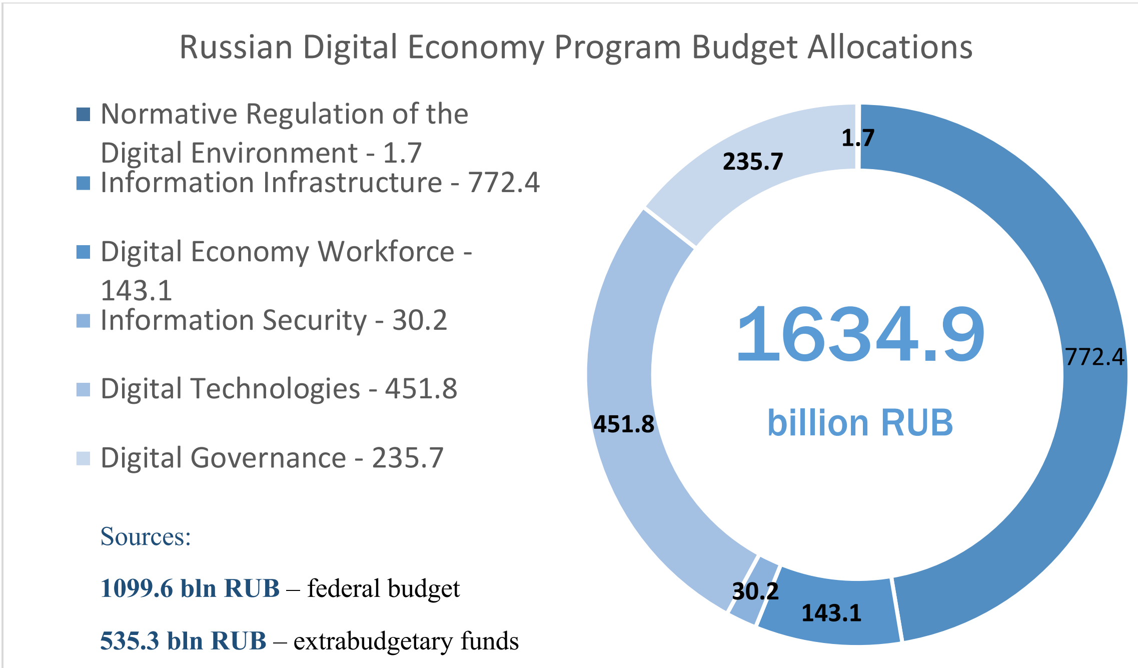

Figure 4. Government budget allocations for Russia's "Digital Economy" program

In a 2020 meeting with deputy heads of federal executive bodies responsible for digital transformation, Russia's current Prime Minister Mikhail Mishustin said that the government needs to create "digital special forces" within the government that would be tasked with addressing global issues facing the country.[305] According to Mishustin, Russia's digital transformation was of special importance, and its success would depend on how quickly the government would be able to utilize the latest technologies: "We need special people for this, with special skills and special experience, if you will, the government's 'digital special forces.' Therefore, the requirements for you are also special," said the prime minister.[306] Comparing digital data with natural resources, he

[305] "Vstrecha Mihaila Mishustina s zamestitelyami rukovoditelei federalnyh organov ispolnitelnoi vlasti, otvetstvennymi za cifrovuu transformaciu [Mikhail Mishustin's meeting with deputy heads of federal executive bodies responsible for digital transformation]." Government of the Russian Federation. March 12, 2020. Accessed July 30, 2022. http://government.ru/news/39129/
[306] See "Mikhail Mishustin's meeting with deputy heads…"

said that it is “the new oil, gold, platinum of the twenty-first century,” only inexhaustible.[307] Mishustin promised to grant the new “digital special forces” special powers to change work processes within their ministries and departments in order to modernize and digitize their government systems.

However, like many Russian government initiatives, the digital special forces failed to deliver desired outcomes. As a result, the following year saw a series of terminations among deputy heads of various departments who failed to meet their obligations under the digital transformation program.[308] “This is a signal for the entire digital industry, which is actively gaining momentum today,” said Russia’s Deputy Prime Minister Dmitry Chernyshenko commenting on the news. “It is important to remember that ministries and regional governments must start digital transformation within themselves first, take these issues seriously, given that they are implementing changes in industries across the country,” he added.[309]

E. Creating Advanced IT and InfoSec Solutions for Domestic and International Markets

As follows from my proposition “E,” the Russian government would use the available economic means to invest in the scientific and high-tech industries with the goal of creating advanced IT and InfoSec solutions, goods, and services for domestic and international markets. To test this proposition, the following section examines federal resource allocations toward initiatives that pursued similar goals in the 2011-2021 period.

[307] See “Mikhail Mishustin's meeting with deputy heads…”
[308] “V Rossii nachalis massovye uvolneniya rukovoditelei gosudarstvennoi cifrovoi transformacii [Mass layoffs of heads of the state digital transformation began in Russia].” *C-News.* January 27, 2021. Accessed July 30, 2022. https://www.cnews.ru/news/top/2021-01-27_v_rossii_nachalis_massovye
[309] See *C-News,* “Mass layoffs of heads of state…”

Additionally, the section highlights how Russian state-owned or affiliated companies have been able to expand their IT and InfoSec offerings abroad.

Russia's "Digital Economy" program states that two of its main outcomes should be: the creation of a system of technology startups that would stimulate the development of the digital economy, as well as the creation of at least ten national high-tech companies capable of developing "end-to-end" technologies for the global market.[310] These objectives almost word-for-word match my proposition "E." By 2017, when the Digital Economy program was approved, the Russian government was in its eighth year of building the innovation center "Skolkovo." Located on the western outskirts of Moscow, the one-and-a-half square mile area was meant to become the Russian version of the U.S. Silicon Valley – the birthplace of IT startups and an incubator for the development of new technologies.[311]

In July 2013, Russia's Ministry of Digital Development, Communications, and Mass Media in partnership with the Ministry of Science and Higher Education announced a call for applications for participation in a government program for the creation of special centers for breakthrough IT research.[312] As part of the five-year program, the selected research and higher ed institutions would receive more than 4 billion rubles ($125.6 million in 2013 equivalent) in government financing to conduct research in the fields of bioinformatics, big data analysis, cloud computing, internet of things (IoT),

---

[310] See Order No 1632-r "Digital Economy of the Russian Federation."

[311] Evgeny Chesnokov. "Skolkovo Stroitsya [Skolkovo is being built]." *Russkiy Bloger* [*Russian Blogger*]. July 3, 2018. Accessed July 30, 2022. https://rblogger.ru/2018/07/03/skolkovo/

[312] Elina Kirillova. "Zapuskaetsya programma po sozdaniyu issledovatelskih centrov v oblasti IT [A program is being launched to create research centers in the field of IT]." *RB.ru*. July 31, 2013. Accessed July 31, 2022. https://rb.ru/news/Zapuskaetsya-programma-po-sozdaniyu-issledovatelskih-centrov-v-oblasti-it/

human-machine interfaces, etc.[313] By November of that same year, the two ministries selected nineteen institutions to become part of the program. In total, according to Minister of Communications and Mass Media Nikolai Nikiforov, the government planned to create up to fifty such research centers.

In August 2013, then-President Dmitry Medvedev signed the federal budget for the construction of Skolkovo over the next seven years. The government allocated 125.2 billion rubles (or $3.93 billion in 2013 equivalent) for the project through 2020, with at least 50 percent of that amount planned to come from private-sector investments.[314] Despite being bogged down in numerous corruption scandals over the years, Skolkovo continued its development.[315] Today, the innovation center includes four so-called "clusters" – conglomerations of private companies and research centers that focus on four corresponding areas of innovation:

1. Cluster of biomedical technologies
2. Cluster of energy-efficient technologies
3. Cluster of information and computer technologies
4. Cluster of space, telecommunications, and nuclear technologies[316]

[313] "Vybrany centry proryvnyh IT-issledovaniy, kotorye poluchat gospodderzhku [Centers for breakthrough IT research have been selected to receive state support]." *C-News*. November 27, 2013. Accessed July 31, 2022. https://www.cnews.ru/news/top/vybrany_tsentry_proryvnyh_itissledovanij
[314] Rasporyazhenie ot 13 avgusta, 2013 g. N 1414-r "O dopolnenii gosudarstvennoi programmy 'Ekonomicheskoe razvitie i inovacionnaya ekonomika' [Order from August 13, 2013, No 1414-r "On expansion of the state program 'Economic development and innovative economy'"]." Government of the Russian Federation. Accessed July 30, 2022. http://government.ru/docs/3843/
[315] Yana Belyaeva. "'Skolkovo': chto vyshlo iz proekta rossiyskoy Kremnievoy doliny ['Skolkovo': what came of the Russian Silicone Valley project]." *Deutsche Welle (DW).* October 27, 2019. Accessed July 30, 2022. https://bit.ly/3DYrH68
[316] "The Clusters." Skolkovo Foundation. Accessed July 30, 2022. https://old.sk.ru/foundation/about/p/clusters.aspx

The cluster of information and computer technologies works on the development of cybersecurity, big data, artificial intelligence, mobile apps, navigation and GPS, and other new systems.[317] As of this writing, the Skolkovo development program was continued through 2024 with annual government financing in the amount of 11.2 billion rubles ($165.8 million in 2022).[318] However, given the severe international sanctions faced by Russia for its war in Ukraine, the future of Skolkovo as the hotbed of Russian IT innovation remains uncertain.

Despite this uncertainty, many Russian companies have been able to expand their IT and InfoSec offerings abroad. Notably, between 2017-2019, several Russian government-affiliated cybersecurity companies signed agreements for providing cybersecurity services to foreign states, including Brazil, the Philippines, Kazakhstan, Vietnam, and North Korea.[319] For example, in 2017, the MePHI Institute, a Russian state-owned nuclear research university, signed a deal to provide cybersecurity equipment and services for Brazil's largest water supply and waste management company.[320]

That same year, Russian cybersecurity firm Solar Security signed a memorandum of partnership and cooperation in promoting cybersecurity services with Kazakhstan's

---

[317] "Klastery 'Skolkovo' [The Clusters of 'Skolkovo']." Skolkovo Foundation. Accessed July 30, 2022. https://sk.ru/foundation/clusters/itc/

[318] "'Interfaks' soobschil o planah Minfina vydelit 'Skolkovo' ewe 45 milliardov rublei [Interfax announced the plans of the Ministry of Finance to allocate another 45 billion rubles to Skolkovo]." *Vedomosti*. September 7, 2018. Accessed July 30, 2022. https://www.vedomosti.ru/economics/news/2018/09/07/780265-skolkovo

[319] The Philippines: "DICT, Russian company to cooperate on cybersecurity initiatives." Republic of the Philippines Department of Information and Communications Technology. September 25, 2018. Accessed January 11, 2023. https://dict.gov.ph/dict-russian-company-to-cooperate-on-cybersecurity-initiatives/; North Korea: "Russian firm provides new internet connection to North Korea." Reuters. October 2, 2017. Accessed January 11, 2023. https://www.reuters.com/article/us-nkorea-internet-idUSKCN1C70D2

[320] Luiz Padilha. "Brasil compra inovação russa para proteção de empresas contra ataques cibernéticos [Brazil buys Russian innovation to protect companies from cyberattacks]." *Defesa Aerea & Naval [Air and Sea Defense]*. July 20, 2017. Accessed January 11, 2023. http://www.defesaaereanaval.com.br/brasil-compra-inovacao-russa-para-protecao-de-empresas-contra-ataques-ciberneticos/

state-owned telecommunications provider Kazakhtelecom.[321] The partnership provided for the creation of a center for monitoring and responding to cyberattacks. A year later, Solar Security was acquired by Russian state-owned telecommunications company Rostelecom.[322] In 2019, Russian cybersecurity firm Kaspersky Lab signed a contract with the government of Vietnam for creating antivirus software for government agencies and critical information infrastructure facilities.[323] While Kaspersky Lab is privately owned, the U.S. government has accused the company of close ties with Russian intelligence agencies.[324]

These deals are congruent with Russia's expected behavior of creating, developing, and implementing Russian IT and InfoSec solutions, both domestically and abroad, which is described in my proposition "E." It is also possible that the Kremlin is trying to expand its access to more countries' cybersecurity systems as a way to create strategic deterrence opportunities. The Russian *Military Doctrine* of 2014 underscores the importance of "the strategic presence of the Russian Federation in world markets for high-tech products and services" while its *Strategy of National Security* of 2015 talks about developing informational measures to ensure strategic deterrence.[325] Russian

---

[321] "AO 'Kazahtelekom' i Solar Security podpisali memorandum o partnerstve i vzaimodeistvii v oblasti kiberbezopasnosti [Kazakhtelecom and Solar Security signed a memorandum of partnership and interaction in the field of cybersecurity]." Rostelekom-Solar*,* April 27, 2017. Accessed January 11, 2023. https://rt-solar.ru/events/news/906/

[322] Igor Lyapunov, Biography. Roskongress. Accessed January 11, 2023. https://roscongress.org/speakers/lyapunov-igor/biography/

[323] "Rossiyskaya kompaniya pomozhet V'etnamu v sozdanii antivirusa dlya gosorganov [Russian company will help Vietnam create antivirus for government agencies]." Ministry of Digital Development, Telecommunications and Mass Media of the Russian Federation. August 7, 2019. Accessed January 11, 2023. https://digital.gov.ru/ru/events/39250/

[324] Jordan Robertson and Michael Riley. "Kaspersky Lab Has Been Working With Russian Intelligence." *Bloomberg.* July 11, 2017. Accessed January 11, 2023. https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence

[325] *Military Doctrine…* Article III, Section 52; Doctrine of Information Security… Article IV, Section 25, Clause b).

military scientists have also repeatedly noted how governments can leverage domestically produced commercial software in their own military-political interests. For example, Kiselev and Kostenko argue that the majority of U.S.-produced software purposefully includes vulnerabilities that, when necessary, can be exploited by U.S. intelligence agencies in order to disrupt the adversary's computer systems.[326] Moscow may pursue similar aims with its efforts to gain access to more countries' cybersecurity systems. While I lack definitive confirmation of Russia's intent, such a focus on providing its own InfoSec solutions to foreign states may be a way for Moscow to create backdoors to their critical infrastructure in order to strengthen Russia's cyberattack capabilities in the event of a confrontation.

F. Leveraging Spheres of Culture and Education

In my proposition "F," I posit that, to defend against the perceived threat of the subversive foreign information influence and discrimination of the Russian language abroad, the Russian government would promote traditional moral, spiritual, and patriotic values among its citizens, as well as the study of the Russian language abroad by using the social-psychological means of culture and education. Therefore, I split the following section into two subsections, each testing the aforementioned proposition by examining the Kremlin's observable actions in the respective spheres of Russian society.

[326] V. Kiselev and A. Kostenko. "Kibervoyna kak osnova gibridnoy operatsii [Cyberwar as the Basis of Hybrid Operations]." *Armeiskii Sbornik* 257, no. 11 (November 2015):3–6. Accessed January 11, 2023. http://www.oboznik.ru/?p=45314

1. Russia's Actions in the Sphere of Education

Russia's "Education Development" program for 2013-2020 was approved by Prime Minister Medvedev on November 22, 2012.[327] In total, the Kremlin allocated nearly 3,8 trillion rubles (or approximately $73.7 billion, based on average annual foreign exchange rates for those years) to the initiative that was scheduled to be implemented in three phases: 2013-2015; 2015-2018; and 2019-2020.[328] The "Education Development" program consisted of several subprograms and federal target programs, including the following:

- Subprogram 1: "Implementation of vocational education programs"
- Subprogram 2: "Promotion of the development of preschool and general education"
- Subprogram 4: "Development of additional education for children and implementation of youth policy activities"
- Subprogram 5: "Improvement of the management of the education system"
- Federal target program "Russian language" 2011-2015
- Federal target program "Russian language" 2016-2020
- Federal target program for the development of education for 2016 – 2020

Subprogram 2, among other targets, aimed at creating conditions for the study of the Russian language by Russian children living abroad. The latter goal was to be accomplished by way of promoting such resources as "Russian Electronic School," an

[327] Rasporyazhenie ot 22 Noyabrya 2012 g. No 2148-r: "Ob utverzhdenii gosudarstvennoy programmy Rossiyskoy Federacii 'Razvitie obrazovaniya' na 2013-2020 gody [Decree of November 22, 2012, No 2148-r: "On approval of the government program of the Russian Federation 'Education Development' for 2013-2020"]." Government of the Russian Federation. Accessed January 11, 2023. http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf 9
[328] See Decree N 295.

online platform providing interactive video classes for all K-12 subjects.[329] Subprogram 4 was tasked with instilling traditional moral values in the younger generation. Its goal was to increase the number of youths taking part in events and activities dedicated to patriotic education.[330]

It is worth emphasizing here that for the Russian State, patriotic education is part of the overall InfoSec strategy. As mentioned earlier in this thesis, Russia's *Military Doctrine* of 2014 highlights the use of ITs to undermine the country's historical, spiritual, and patriotic traditions as one of the main InfoSec risks facing the nation.[331] According to Russian military scientists, the dissolution of the Soviet Union opened the doors to the flow of destructive information, coming from the West, that threatens Russia's national security.[332] Part of this destructive influence is directed at the erosion of traditional spiritual and moral values among the Russian youths. The perceived goal behind this negative influence is, of course, to discredit the Russian government and destabilize the political situation within the country. As a result, the Kremlin sees patriotic education as a way to counter information-psychological threats coming from the West. The government believes that such education can influence the worldview, as well as the moral and psychological standing of the nation, and therefore, it is fundamental to assuring Russia's information security.

329 Decree N 295, pp. 20-23.
330 Decree N 295, p. 26.
331 *Military Doctrine*… Article II, Section 13, Clause c).
332 Aleksandr G. Likhonosov. "Schastie – luybit svou rodinu. Patrioticheskoe vospitanie grazhdan strany kak osnova informacionnoy bezopasnosti gosudarstva [Happines is to love your homeland! Patriotic education of citizens of the country as the basis of information security of the state]." *Vestnik Voennogo Obrazovaniya* [*Military Education Courier*]. May-June 2021 No.3 (30). Accessed July 31, 2022. https://bit.ly/3lCG6yv

As an integral part of social and cultural identity and the primary mode of communication between people, language is central to Russia's goal of unifying its society behind common spiritual and moral values. Federal target program "Russian language" focused on promoting and spreading the Russian language and culture, as well as making education in Russian more accessible to compatriots living abroad. According to the program, the Russian language is to serve as a soft-power means for consolidating Russian society and increasing the country's geopolitical influence, including in the CIS.[333]

To accomplish these ends, in addition to printing and disseminating Russian textbooks, the government planned to introduce software and methodological support for using remote learning technologies in teaching the Russian language abroad. As one of its targets, the program aimed at increasing the number of information resources for studying the Russian language by 170 percent between 2011-2015. For the 2016-2020 period, the program planned for a tenfold increase in the number of online resources, allowing both Russians and foreigners to study the Russian language and receive information about Russian culture.[334]

On May 29, 2014, the head of the Russian Association for International Cooperation, Sergei Stepashin, declared that compulsory study of the Russian language was introduced in all Syrian schools.[335] On November 14, 2017, Russian news media reported that the Iraqi Ministry of Education added Russian to the list of school

---

[333] Decree N 295, p. 40.
[334] Decree N 295, p. 56.
[335] "V shkolah Sirii vvedeno obyazatelnoye izuchenie russkogo yazyka [Compulsory study of the Russian language introduced in Syrian schools]." *RIA Novosti* [*RIA News*]. May 29, 2014. Accessed July 31, 2022. https://ria.ru/20140529/1009878505.html

subjects.[336] On February 14, 2018, similar reports alleged that the Russian language would soon be taught in several schools in Cuba.[337]

2. Russia's Actions in the Sphere of Culture

To help further unify Russian society around traditional moral and spiritual values, the Russian government added "Culture Development" to its list of national projects. Planned for the period of 2013-2020, the project was aimed at "strengthening the unity of Russian society and Russian civic identity, increasing the number of citizens involved in cultural activities, and increasing the demand for digital resources in the field of culture."[338] Just like Russia's "Education Development" program for the same period, this project consisted of several subprograms and federal target programs, such as "Russian culture" (2012-2018), and "Strengthening the unity of the Russian nation and the ethno-cultural development of the peoples of Russia" (2014-2020).

Both of these target programs leveraged ITs to accomplish their goals. For example, the "Russian culture" program paid special attention to the goal of digitizing the sphere of Russian culture and equipping organizations that carry out educational activities in the fields of culture and art with modern technical means. Some of the program's targets included increasing the share of cultural institutions that have their own

[336] "V irakskih shkolah nachnut izuchat' russkiy yazyk [Iraqi schools to begin teaching Russian language]." *RIA Novosti* [*RIA News*]. November 14, 2017. Accessed July 31, 2022. https://ria.ru/20171114/1508770850.html
[337] "V dvuh Kubinskih shkolah nachnut prepodavat' russkiy yazyk [Russian language will be taught in two Cuban schools]." TASS. February 15, 2018. Accessed July 31, 2022. https://tass.ru/obschestvo/4959319
[338] Postanovlenie Pravitelstva RF ot 15 aprelya 2014 g. N 317 "Ob Utverzhdenii gosudarstvennoy programmy Rossiyskoy Federacii 'Razvitie kultury' [Decree of the Government of the Russian Federation of April 15, 2014, N 317 "On approval of the state program of the Russian Federation 'Development of culture'"]." Government of the Russian Federation. Accessed July 31, 2022. http://gov.garant.ru/SESSION/PILOT/main.htm

web portals; increasing the number of bibliographic records in the electronic catalog of Russian libraries; and increasing the share of Russian-made movies in the domestic market to 28 percent.[339] In total, the government allocated nearly 147 billion rubles to the program over its six-year period (or $2.04 billion in 2020).

The program dedicated to unifying Russian society, however, was even more ambitious, receiving nearly 85 trillion rubles over its six-year period (or $1.81 trillion in 2020).[340] Aimed at strengthening civil unity and "harmonizing" interethnic relations within Russia's multinational society, the initiative was tasked with implementing a nationwide propaganda campaign that would use all forms of mass media, including the internet. The campaign would involve the production and distribution of patriotic content via TV and radio channels, as well as "the creation of thematic radio and television programs, newspaper and magazine columns, Internet projects, the publication and supply of textbooks, teaching aids, fiction, popular science, reference literature, and multimedia publications."[341]

By 2020, Russia's "Culture Development" project led to the creation of "Culture.RU" ("Культура.РФ"), a web portal that popularizes Russian cultural heritage, as well as the National Electronic Library, an online resource that provides digital access to full texts of Russian books, museum collections, and archival documents.[342] According

339 See Decree N 317…
340 See Decree N 317…
341 Postanovlenie Pravitelstva RF ot 20 avgusta 2013 g. N 718 "O federalnoy celevoy programme 'Ukrepleniye edinstva rossiyskoy nacii i etnokulturnoe razvitie narodov Rossii (2014-2020 gody)' [Decree of the Government of the Russian Federation of August 20, 2013, N 718 "On the federal target program 'Strengthening the unity of the Russian nation and the ethno-cultural development of the peoples of Russia (2014 - 2020)'"]." Government of the Russian Federation. Accessed July 31, 2022. https://base.garant.ru/70439260/
342 Postanovlenie Pravitelstva Rossiyskoy Federacii ot 01.11.2021 g. No.1897 [Government of the Russian Federation resolution of November 1, 2021, No.1897]. Government of the Russian Federation. Accessed July 31, 2022. http://government.ru/docs/all/137420/

to the Ministry of Culture, in 2020, the number of visits to Russian digital resources in the sphere of culture exceeded 182 million, a 100 percent increase over 2019.[343] The Russian movie industry also received a strong boost. In the first half of 2020, the share of Russian-made movies in the domestic market exceeded 52 percent.[344] It should be noted, however, that the global coronavirus pandemic played a significant part in increasing these numbers. With most public venues shut down due to the virus, most people had no other choice but to turn to television or go online for their entertainment needs.

G. Building Russian Information Ecosystem

According to my proposition "G," to further defend against foreign information influence, the discrimination of the Russian media, and biased assessments of Russian policy abroad, the Russian government would employ its economic means to create state-funded media and information resources that would provide both domestic and international audiences with the Kremlin's point of view on Russian policies and world events. To test this proposition, I analyzed Russia's resource allocations to several federal programs aimed at developing nationwide information infrastructure, creating state-funded media and information resources, preventing information threats, and increasing Russia's presence in the international information environment.

Russia's main government initiative for the development of nationwide information infrastructure, mass media, and the prevention of information threats, was

---

[343] See resolution No.1897…

[344] "Dolya rossiyskogo kino v obwem prokate vpervye prevysila dopandemiynyi pokazatel [The share of Russian cinema in general distribution for the first time exceeded the pre-pandemic figures]." *Sostav.ru.* July 19, 2021. Accessed July 31, 2022. https://www.sostav.ru/publication/rossijskoe-kino-rost-prokata-49480.html

approved in 2011 as part of its "Information Society" program.[345] Initially, the program also aimed to make Russia less dependent on imported IT. However, by 2016, that goal was abandoned "due to the lack of funding required to achieve it."[346] With a planned budget of 1.2 trillion rubles ($40.9 billion in 2011), the program was to be implemented in two stages: 2011-2014 and 2015-2020. It was comprised of the following subprograms: [347]

- "Information and telecommunications infrastructure of the information society and services provided on its basis"
- "Information State"
- "Security in the information society"
- "Information environment"

As evident from its name, the "Information and telecommunications infrastructure […]" subprogram was tasked with establishing the technological foundation needed for the formation of an internet-connected society. One of the subprogram's targets was to increase the share of households with broadband access to the internet from 34 percent in 2010 to 95 percent in 2020.[348] Of course, building this information infrastructure required a massive investment in the physical infrastructure in the form of high-speed fiber-optic

---

[345] Rasporyazhenie Pravitelstva RF ot 2 dekabrya 2011 g. No 2161-r: "Gosudarstvennaya programma Rossiyskoy Federacii 'Informacionnoe Obwestvo' (2011-2020 gody) [Decree of the Government of the Russian Federation of December 2, 2011, N 2161-r: "Government program of the Russian Federation 'Information Society' (2011 - 2020)"]." Government of the Russian Federation. Accessed July 31, 2022. http://www.pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102142714&backlink=1&&nd=102152835

[346] "Iz gosprogrammy 'Informacionnoe obwestvo' udalyaut punkt o tehnologicheskoy nezavisimosti Rossii [The item on the technological independence of Russia is removed from the state program 'Information Society']." *C-News.* December 28, 2016. Accessed July 31, 2022. https://www.cnews.ru/news/top/2016-12-28_minkomsvyazi_otkazalos_ot_dostizheniya_tehnezavisimosti

[347] See Decree N 2161-r: "Information Society" program.

[348] See Decree N 2161-r: "Information Society" program.

communication lines capable of transmitting large amounts of data over long distances. In 2014, Russia's state-owned telecommunications company Rostelecom finished its nearly 2,200-mile-long fiber-optic communication line called "Northern Optical Flow."[349]

One of the largest of such projects in Russia over the past eleven years, the Northern Optical Flow stretches between Yekaterinburg and Salekhard, connecting some of the largest cities in Russia's Ural region. The cost of the project is estimated at 10 billion rubles ($265 million in 2014).[350] After its launch, internet speeds in the region increased by up to twenty times while costs to access the web went down.[351] The same communication line was then laid in Russia's westernmost region of Kamchatka.[352] By 2019, 16 of 19 thousand Russian settlements with a population between 500 and 10 thousand people, as well as 8 of 14 thousand settlements with a population between 250 and 500 people, received access to broadband internet.[353]

Subprogram "Information State" aimed at digitizing the Russian government and increasing the amount of government services citizens can receive online. According to this subprogram, by 2020, Russian citizens would be able to receive the majority of federal and municipal government services, including in such areas as healthcare,

---

[349] "'Rostelekom' podvel itogi ekspluatacii Severnogo opticheskogo potoka [Rostelecom summed up the operation of the Nord Optical Stream]." *C-News*. April 14, 2016. Accessed July 31, 2022. https://www.cnews.ru/news/line/2016-04-14_rostelekom_podvel_itogi_ekspluatatsii_severnogo

[350] "'Rostelekom' vlozhil bolee 10 mlrd rublei v liniyu svyazi ot Ekaterinburga do Saleharda [Rostelecom invested more than 10 billion rubles in a communication line from Yekaterinburg to Salekhard]." TASS. April 15, 2014. Accessed July 31, 2022. https://tass.ru/ekonomika/1121596/amp

[351] *C-News*, "Rostelecom summed up the operation…"

[352] "Podvodnaya VOLS Kamchatka-Sahalin-Magadan [Underwater fiber optic communication line (FOCL) Kamchatka-Sakhalin-Mgadan]." Rostelecom. Accessed July 31, 2022. https://www.company.rt.ru/projects/digital_economy_rf/focl/FarEast_FOCL/

[353] Rostelecom, "Underwater fiber optic communication…"

education, science, and culture, in the digital form.[354] Indeed, Russia has made significant progress in this regard. Today, Russian citizens can receive a variety of government services, such as applying for a passport or driver's license, paying taxes and traffic fines, or making a doctor's appointment, by using the web portal Gosuslugi.ru (the word "gosuslugi" is a portmanteau of the Russian words "government" and "services"). By the end of 2019, more than 100 million Russians have created personal accounts in the portal.[355] The project was so successful that, by the end of 2018, the UN ranked Russia at number 32 in the world in terms of the level of development of its "electronic government" – that is, digital interaction between government, organizations, and citizens.[356] At the same time, Moscow ranked as the world leader among individual cities.

Meanwhile, the subprogram "Security in the information society" focused on monitoring potential information threats and ensuring proper protection of the various components in the digital infrastructure network. This included regulation, licensing, and registration of various activities in the fields of communications, ITs, and mass media.[357]

However, the lion's share of the "Information Society" program's budget – nearly 588 billion rubles ($20 billion in 2011) – was allocated to the "Information environment" subprogram. Its goals were to ensure that all Russian citizens can receive the Kremlin's point of view on events in the country and the world.[358] A particular emphasis was made on growing domestic media content pertaining to traditional cultural, moral, and family

[354] See Decree N 2161-r: "Information Society" program.
[355] "Chislo polzovateley portala gosuslug priblizilos k sta millionam [The number of users of the government services portal approached one hundred million]." *RIA Novosti* [*RIA News*]. October 17, 2019. Accessed July 31, 2022. https://ria.ru/20191017/1559902373.html
[356] UN E-Government Survey 2018. United Nations. Accessed July 31, 2022. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018
[357] See Decree N 2161-r: "Information Society" program.
[358] See Decree N 2161-r: "Information Society" program.

values. At the same time, information that contradicts the government's vision was to be restricted.

The subprogram was also tasked with increasing Russia's presence in the international information environment. This was to be accomplished primarily by way of providing support to Russian-language international media. For instance, one of the subprogram's targeted goals was to increase the audience of the *Russia Today* channel from 400 million viewers in 2010 to 580 million in 2020.[359]

Indeed, digital mass media play a major role in Russia's information security strategy. Television in particular has traditionally been the most trusted and accessible form of mass media for Russian citizens.[360] As such, it has always been part of Moscow's InfoSec strategy and played a central role in the way the Kremlin shapes and controls the domestic information environment. All major TV channels in Russia are either directly owned by the government or otherwise controlled through ownership by government-affiliated entities. Every year, the Kremlin allocates tens of billions of rubles to support its mass media apparatus.

In 2011, the government reclassified mass media into its own federal budget item after previously grouping them with culture and cinematography.[361] Even during the Russian financial crisis of 2014-2016, when the government was cutting its social spending and freezing state-funded pension contributions, the Kremlin continued to

---

[359] See Decree N 2161-r: "Information Society" program.
[360] Yana V. Shvec. "Vliyanie televidiniya na informacionnoe prostranstvo sovremennoy Rossii [The influence of television on the information space of modern Russia]." *Bulletin of the Volga Region Institute of Administration.* 2018. Vol.18 No.2. Accessed July 31, 2022. https://cyberleninka.ru/article/n/vliyanie-televideniya-na-informatsionnoe-prostranstvo-sovremennoy-rossii
[361] Annual information on the execution of the federal budget (data from January 1, 2006). The Russian Ministry of Finance. June 27, 2022. Accessed July 31, 2022. https://minfin.gov.ru/ru/statistics/fedbud/execute/?id_65=80041-yezhegodnaya_informatsiya_ob_ispolnenii_federalnogo_byudzhetadannye_s_1_yanvarya_2006_g

increase its funding for mass media.[362] For example, in 2015, the government increased its subsidies for the TV channel *Russia Today* (*RT*) by nearly 30 percent, while funding for its parent company, the international information agency *Russia Today*, was increased by a whopping 250 percent.[363]

In 2017, Moscow increased its mass media subsidies yet again. The additional 2.5 billion rubles ($43 million in 2017) went to such entities as Russia's state news agency *TASS* (₽900 million or $15.5 million), international information agency *Russia Today* (₽792 million or $13.6 million), and the country's largest media corporation the *Russian Television and Radio Broadcasting Company* (*RTR*) (₽186 million or $3.2 million).[364] Overall, government financing of mass media nearly doubled between 2011 and 2020.

Table 1. Russian federal budget allocations 2010-2021

Russian Federal Budget Allocations (bln RUB)												
Sector	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021****[**]**
National issues (including servicing of government and municipal debt)*	887.9	777.8	809.9	850.07	935.07	1,117.07	1,095.6	1,162.4	1,257.1	1,363.5	1,507.7	1,766.6
	195.0											
Servicing of government and municipal debt		262.7	320.0	360.3	415.06	518.7	621.3	709.2	806.0	730.8	784.2	1,084.2
National Defense	1,276.5	1,516.0	1,812.4	2,103.6	2,479.1	3,181.4	3,775.3	2,852.3	2,827.0	2,997.4	3,168.8	3,576.1
National Security and law enforcement	1,085.4	1,259.8	1,843.0	2,061.6	2,086.2	1,965.6	1,898,7	1,918.0	1,971.6	2,083.2	2,226.6	2,337.7
National economy	1,222.7	1,790.2	1,968.5	1,849.3	3,062.9	2,324.2	2,302.1	2,460.1	2,402.1	2,827.1	3,483.9	4,356.7

362 Olga Kuvshinova. "Pravitelstvo v tretiy raz zamorozilo nakopitelnye pensionnye vznosy [The government froze funded pension contributions for the third time]." *Vedomosti.* September 29, 2015. Accessed July 31, 2022. https://www.vedomosti.ru/economics/articles/2015/09/29/610770-pravitelstvo-medvedeva-zamorozilo

363 "V 2015 godu telekanal Russia Today poluchit na 41% bolshe subsidiy [In 2015 TV channel Russia Today will receive 41% more government subsidies]." *RBC.ru*. September 23, 2014. Accessed July 31, 2022. https://www.rbc.ru/politics/23/09/2014/5704227a9a794760d3d41a87

364 Farida Rustamova. "Budzhet gosudarstvennyh SMI v Rossii vyrastet na 2,5 milliarda rubley [The budget of state media in Russia will grow by 2.5 billion rubles]." *The BBC*. May 26, 2017. Accessed July 31, 2022. https://www.bbc.com/russian/news-40062877

Department of housing and utilities	234.9	279.8	228.8	177.5	119.6	144.1	72.2	119.5	148.8	282.2	371.5	591.4
Environmental protection	13.5	17.6	22.5	24.3	46.4	49.7	63.1	92.4	116.0	197.6	260.6	405.01
Education	442.8	553.4	603.8	672.3	638.3	610.6	597.8	615.0	722.6	826.5	956.9	1,064.6
Culture, cinematography, and mass media*	125.6											
Culture and cinematography		83.8	89.9	94.8	97.8	89.9	87.3	89.7	94.9	122.4	144.5	146.7
Mass media		61.1	77.5	77.3	74.8	82.1	76.6	83.2	88.4	103.5	121.1	114.0
Healthcare and sport*	347.4											
Healthcare		499.6	613.8	502.0	535.5	516.0	506.3	439.8	537.3	713.0	1,334.4	1,474.0
Physical culture and sport		44.2	45.7	68.0	71.2	73.0	59.6	96.1	64.0	81.4	75.3	70.9
Social policy	344.9	3,128.5	3,859.7	3,833.1	3,452.4	4,265.3	4,588.5	4,992.0	4,581.8	4,882.8	6,990.3	6,675.9
Interbudgetary transfers*	4,135.9											
General interbudgetary transfers to budgets of the Russian budgetary system		651.3	599.4	668.1	816.1	682.0	672.0	790.7	1,905.4	1,003.1	1,395.9	1,107.7

** - Functional spending classification used before 2011*
*** - Preliminary data*

When it comes to international information campaigns, digital news outlets *RT* and *Sputnik* serve as Russia's primary megaphones broadcasting Moscow's point of view on world events and news of the day. Propped by generous government funding, both *RT* and its sister agency drastically grew their digital footprint in my research period.[365] Since 2011, *RT* and *Sputnik* have opened offices in key regions around the world, including the U.S., China, France, Germany, and Egypt, publishing news in more than thirty different languages. Thanks to its accessibility, and broad language support, by 2020, *Sputnik* had become the most popular Russian state-sponsored media outlet in the

[365] "Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem." U.S. Department of State Global Engagement Center Special Report. January 2022. Accessed July 31, 2022. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf

Balkans.[366] As of 2021, *RT* offered broadcasts in English, Arabic, Spanish, French, German, and Russian, and had an established presence in Europe, the Middle East, and Latin America.[367] In recent years, the Kremlin has also signed several media cooperation agreements with African countries, thus expanding the Russian influence on the continent.[368]

While *RT* and *Sputnik* describe their content as mere "alternative views to the mainstream media," Western governments have widely accused the two news agencies of conducting covert disinformation campaigns at the behest of Russian intelligence services.[369] Despite their growth, however, *RT* and *Sputnik*'s audience remains a far cry from more established international channels like *CNN* or *BBC*. Nevertheless, thanks to their intentionally polarizing content and a massive army of automated bot followers on social media, both agencies were able to create a highly effective information warfare machine that continues to sow skepticism of Western narratives while promoting those that benefit the Russian government.[370]

H. Developing Russia's Own Means of Information Influence on Public Opinion Abroad

---

[366] Atlantic Council of Montenegro. "Russia's Narratives Toward the Western Balkans: Analysis of Sputnik Srbija." NATO Strategic Communications Centre of Excellence. April 2020. ISBN: 978-9934-564-24-6. Accessed July 31, 2022. https://stratcomcoe.org/publications/russias-narratives-toward-the-western-balkans-analysis-of-sputnik-srbija/56

[367] See: U.S. Department of State, "Kremlin-Funded Media…"

[368] Nataliya Bugayova et al. "The Kremlin's Inroads after the Africa Summit." Institute for the Study of War. November 8, 2019. Accessed January 15, 2023. http://www.understandingwar.org/backgrounder/kremlins-inroads-after-africa-summit

[369] Steven Erlanger. "Russia's RT Network: Is It More BBC or K.G.B.?" *The New York Times.* March 8, 2017. Accessed July 31, 2022. https://www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html; Also, see U.S. Department of State, "Kremlin-Funded Media…"

[370] Jim Rutenberg. "RT, Sputnik and Russia's New Theory of War." *The New York Times*. September 13, 2017. Accessed July 31, 2022. https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html

My proposition "H" is that the Russian government would work on developing its own effective means of information influence on public opinion abroad. This measure was proposed in Russia's 2013 and 2016 *Foreign Policy Concepts*. I test this proposition in this section by investigating the open-source record of Russia's information-psychological operations in 2011-2021, including the role of the Russian Internet Research Agency and the Federal News Agency in carrying out disinformation campaigns both domestically and abroad.

Since 2011, Russia has invested enormous resources to adapt its Soviet-era information confrontation tactics to the digital age. Besides creating a state-funded media conglomerate to provide both domestic and international audiences with the Kremlin's point of view, the Russian government has adopted social media technologies as effective means of exerting information influence on public opinion. Today, the massive social media amplifier relied upon by the Russian IW machine is made up of an increasingly complex and well-organized network of computer bots, online forums, fake news sites, and government-paid anonymous commentators known as "trolls."[371] While bots can be programmed to "like" and "share" desired narratives on social media, trolls are used to engage with and agitate target audiences on a broad set of issues and in multiple languages.

Such information-psychological influence operations were made possible through the so-called "troll factories." Perhaps the first and the most well-known of them is the Internet Research Agency in St. Petersburg, Russia. In 2013, an investigation by Russian newspaper *Novaya Gazeta* revealed that the agency was owned by Yevgeny Prigozhin, a

[371] Giles, "Russia's 'New' Tools…"

Russian oligarch with close ties to Vladimir Putin and founder of the infamous private military company the Wagner Group that would participate in the Russo-Ukrainian War that Russia would initiate in 2022.[372] According to leaked email correspondence, as of 2014, Prigozhin invested 33.5 million rubles per month (or nearly $1 million in 2014 exchange rates) into his media resource.[373] Located in a modern four-story building, the agency was staffed with hundreds of writers, translators, and IT specialists who worked around the clock to support and amplify government disinformation and propaganda operations, both domestically and abroad.[374]

In 2014, the Internet Research Agency was joined by the Federal News Agency, which was often referred to as the "media factory."[375] The "media factory" and the "troll factory" were united by a common address and leadership – both were said to be owned and funded by Prigozhin, although he continues to deny his affiliation with these entities. By 2017, the Federal News Agency, grew to include sixteen news sites with a monthly audience of more than 33 million people – more than some of the largest Russian digital news media at the time.[376]

Domestically, the two agencies work in tandem to disseminate government-approved content and thwart opposing opinions. As of the 2011-2021 period, the content

---

[372] Aleksandra Garmazhapova. "Gde zhivut trolli. I kto ih kormit [Where trolls live. And who feeds them]." *Novaya Gazeta* [*New Gazette*]. September 7, 2013. Accessed July 31, 2022. https://novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit; also see Pjotr Sauer. "Putin ally Yevgeny Prigozhin admits founding Wagner mercenary group." *The Guardian*. September 26, 2022. Accessed January 15, 2023. https://www.theguardian.com/world/2022/sep/26/putin-ally-yevgeny-prigozhin-admits-founding-wagner-mercenary-group

[373] Denis Korotkov. "Sotni trollei za million [Hundreds of trolls for millions]." *Fontanka.ru.* May 29, 2014. Accessed July 31, 2022. https://www.fontanka.ru/2014/05/29/170/

[374] Dmitry Volchek. "Bezumie, kremlevskih trollei [Madness of Kremlin's trolls]." *Radio Svoboda* [*Radio Freedom*]. March 15, 2015. Accessed July 31, 2022. https://www.svoboda.org/a/26913247.html

[375] Kirill Sokolov. "Rassledovanie RBK: kak iz 'fabriki trolley' vyrosla 'fabrika media' [RBC investigation: how a 'media factory' grew out of a 'troll factory']." *RBC.ru*. March 24, 2017. Accessed July 31, 2022. https://www.rbc.ru/technology_and_media/24/03/2017/58d106b09a794710fa8934ac

[376] Sokolov, "RBC investigation…"

typically included news about the achievements of Vladimir Putin, destabilizing activities of political opposition, as well as government propaganda about the Ukrainian and Syrian conflicts. Separate departments are responsible for posting comments on social media and news sites, writing and publishing blogs, creating video content, and even political memes.[377]

Each day, the agency generates tens of thousands of online comments, which are then multiplied tenfold by an extensive network of computer bot accounts made to look like real people.[378] For instance, on February 27, 2015, just hours after prominent Russian opposition leader Boris Nemtsov was shot dead near the Kremlin, dozens of Twitter accounts began spreading nearly identical posts alleging that the assassination was ordered by Ukrainian oligarchs.[379] After analyzing nearly 20,500 pro-Kremlin Twitter accounts, UK-based open source and social media analyst Lawrence Alexander concluded that the evidence "strongly supports the idea that the bots were created by a common agency – and the weight of evidence points firmly towards Moscow."[380] Other independent investigations by Russian and American journalists identified the Internet Research Agency as the source of the massive disinformation campaign following Nemtsov's assassination.[381]

---

377 Sokolov, "RBC investigation…"

378 For additional details about the number of generated posts, read: Andrey Soshnikov. "Internet-trolli iz Olgino zagovorili na angliyskom i ukrainskom [Internet trolls from Olgino started to speak in English and Ukrainian]." *MR7.ru*. May 30, 2014. Accessed July 31, 2022. https://mr-7.ru/articles/102680/; for more information about the network of computer bots created by the agency, read Lawrence Alexander. "Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign." *GlobalVoices.org*. April 2, 2015. Accessed July 31, 2022. https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/

379 Andrey Soshnikov. "Stolica politicheskogo trollinga [The capital of political trolling]." *MR7.ru*. March 11, 2015. Accessed July 31, 2022. https://mr-7.ru/articles/112478/

380 Alexander, "Social Network Analysis…"

381 Diana Hachatryan. "Kak stat' trollhanterom [How to become a troll hunter]." *Novaya Gazeta* [*New Gazette*]. March 10, 2015. Accessed July 31, 2022. https://novayagazeta.ru/articles/2015/03/10/63342-kak-stat-trollhanterom; also, see Adrian Chen. "Agenstvo [The Agency]." *The New York Times*. June 4, 2015.

Similar tactics are also being employed to influence public opinion outside Russia. As reported by former employees, the troll factory has an entire department staffed with English speakers whose job is to engage in online conversations with European and American citizens. In an interview with the independent Russian television channel TV Rain, a former employee recounted the following:

> "You were given a list of media outlets that you had to monitor and comment on. New York Times, Washington Post – there were tens of thousands of comments. You had to look through all that and understand the general trend, what people write about, what they argue about. And then you had to get into the dispute yourself in order to kindle it, try to rock the boat. […] Our goal was not to turn Americans towards Russia. Our goal was to turn Americans against their own government."[382]

Besides trying to agitate the public in online forums, the Internet Research Agency has carried out elaborate disinformation campaigns in the U.S. For instance, on September 11, 2014, there were widespread allegations that terrorists from the Islamic State blew up a chemical plant in Centerville, Louisiana.[383] The fake news was spread from lookalike clones of *CNN.com*, as well as of local Louisiana news sites. Then, dozens of bogus Twitter accounts began sharing the news with public figures to maximize its exposure.[384]

Among the thousands of other information attacks conducted similarly since 2014 were: false reports of an Ebola virus outbreak in the U.S., rumors of police officers shooting an unarmed African American woman, and numerous conspiracy theories about

---

Accessed July 31, 2022. https://www.nytimes.com/2015/06/07/magazine/the-agency-russian.html#commentsContainer

[382] Evgeniya Kotlyar. "'U nas byla cel'…vyzvat' besporyadki': intervju s eks-sotrudnikom 'fabriki trolley' v Sankt-Peterburge ['We had a goal ... to cause unrest': an interview with an ex-employee of the 'troll factory' in St. Petersburg]." *Telekanal Dojd'* [*TV Rain*]. October 14, 2017. Accessed July 31, 2022. https://tvrain.ru/teleshow/bremja_novostej/fabrika-447628/

[383] Chen, "The Agency."

[384] Chen, "The Agency."

COVID-19.[385] In February 2018, the U.S. government indicted the Internet Research Agency and some of its personnel for "interference operations targeting the United States" with "a strategic goal to sow discord in the U.S. political system, including the 2016 U.S. presidential election."[386] Nevertheless, both the Internet Research and the Federal News Agencies have continued their operations. By December of the same year, the two "factories" moved to a larger office space at the "Lakhta-2" business center in St. Petersburg.[387] It should be noted, however, that a newly released study by the Center for Social Media and Politics at New York University found that the influence of Russian bots on attitudes and voting behavior in the 2016 U.S. presidential election was rather limited, despite the numerous disinformation campaigns conducted by the Internet Research Agency.[388]

I. Controlling Domestic Information Environment

It follows from my proposition "I" that, to prevent the use of ITs to undermine Russia's sovereignty, political and regional stability, the Kremlin would use available legal-administrative means to establish better government control within its information sphere. The following section tests its validity by examining how the Russian

---

385 Chen, "The Agency." Also, see: Bobby Allyn. "Study Exposes Russia Disinformation Campaign That Operated In The Shadows For 6 Years." *NPR*. June 16, 2020. Accessed July 31, 2022. https://www.npr.org/2020/06/16/878169027/study-exposes-russia-disinformation-campaign-that-operated-in-the-shadows-for-6-

386 United States of America v. Internet Research Agency LLC. 18 U.S.C. §§ 2, 371, 1349, 1028A. Case 1:18-cr-00032-DLF. (2018). Accessed July 31, 2022. https://www.justice.gov/file/1035477/download

387 Anna Trunina and Andrey Zaharov. "'Fabrika trolley' pereehala v 'Lahtu-2' [Troll factory moved to Lakhta-2]." *RBC.ru.* December 30, 2017. Accessed July 31, 2022. https://www.rbc.ru/business/30/12/2017/5a465d969a79472a87a3c920

388 Gregory Eady et al. "Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior." *Nature Communications* 14, 62 (2023). Accessed February 6, 2023. https://doi.org/10.1038/s41467-022-35576-9

government used its legal-administrative means in the form of domestic policies during the 2011-2021 research period.

As the Russian troll factories conducted information-psychological operations trying to influence public opinion on a variety of issues, both at home and abroad, the Kremlin went to great lengths to isolate Russian citizens from any unwanted information, starting with independent digital news media. In recent years, one news outlet after another was either closed, blocked, or editorially constrained.

Aiming to limit outside influence on the domestic information environment, on September 23, 2014, the State Duma passed a law curtailing foreign ownership of media outlets. Taking effect in 2017, the law prohibited foreign investors to own more than a 20-percent stake in any Russian media outlet. One of the co-authors of the bill Vadim Dengin characterized the legislation as a matter of national security: "It is necessary to clearly distinguish between the reasons why a person buys a media outlet – to do business or pursue their own policy and change the situation in the country."[389] The law impacted some of Russia's most prominent then-independent publications, including the majority of popular glossy magazines and business newspapers, such as *Forbes, Kommersant*, and *Vedomosti*.[390]

In January 2014, Russia's main opposition TV channel *Dozhd* (*TV Rain*) was cut from the airwaves by most satellite and cable operators following a scandal over an

---

[389] Nadezhda Kasyanova. "Deputaty predlozhili ogranichit' innostrannoe uchastie v rossiyskih CMI [Deputies proposed to limit foreign participation in Russian media]." *E1.ru.* September 17, 2014. Accessed July 31, 2022. https://www.e1.ru/text/gorod/2014/09/17/52892691/

[390] "Putin ogranichil innostrannye doli v rossiyskih SMI [Putin limited foreign stakes in Russian media]." *The BBC.* October 15, 2014. Accessed July 31, 2022. https://www.bbc.com/russian/russia/2014/10/141015_putin_media_foreign

online poll conducted by the TV channel.[391] The poll asked people whether Leningrad (now St. Petersburg) should have been surrendered to save hundreds of thousands of lives during World War II when the city was under a 900-day blockade. After the channel's actions were deemed offensively unpatriotic by several high-ranking government officials, including Vladimir Putin's Press Secretary Dmitry Peskov, *Dozhd*'s modes of broadcasting to viewers in Russia were restricted to internet only, which put it on the brink of bankruptcy.

As the Kremlin continued to tighten its grip on the free Russian media, a month after revoking *Dozhd's* broadcasting license, General Director of the Russian radio station *Echo of Moscow* Yuri Fedutinov – who had held this role since 1992 – was replaced by Ekaterina Pavlova. Pavlova had previously served as the editor-in-chief and deputy chairman of the state-owned radio station *The Voice of Russia*.[392] Then, in March of the same year, Roskomnadzor accused one of the most popular Russian digital news outlets *Lenta.ru* of spreading extremist information after it had published an interview with one of the leaders of a Ukrainian nationalist movement.[393] Within hours, the publication's Editor in Chief Galina Timchenko was replaced. Timchenko immigrated to Latvia shortly after where she launched a new site, *Meduza.io*, which soon became one of the most prominent independent Russian-language news sites.

---

[391] Kseniya Boletskaya and Mari Mesropya. "Operatory otkluchayut 'Dojd' po vsey strane [Operators turn off "Rain" throughout the country]." *Vedomosti.* January 29, 2014. Accessed July 31, 2022. https://www.vedomosti.ru/technology/articles/2014/01/29/operatory-otklyuchayut-dozhd-po-vsej-strane

[392] Natalya Korchenkova. "U 'Eha Moskvy' poyavilsya novyi generalnyi director [Ekho Moskvy has a new CEO]." *Kommersant.* February 18, 2014. Accessed July 31, 2022. https://www.kommersant.ru/doc/2410985

[393] "Lenta.ru protiv uvolneniya glavnogo redaktora [Lenta.ru against the dismissal of the editor-in-chief]." *Radio Free Europe Radio Liberty*. March 13, 2014. Accessed July 31, 2022. https://www.rferl.org/a/25296359.html

On May 5, 2015, President Putin signed a law banning the use of profane language in movies and literature, during concerts and theatrical performances, as well as on TV and in all print and digital news media.[394] Secretary of the Union of Journalists of Russia Ashot Dzhazoyan, characterized the bill as “the death penalty for the media.”[395] A year later, in 2016, Putin signed another restrictive law prohibiting foreign organizations from researching the volume of Russian TV audiences.[396] Western security analysts interpreted the move as a defensive measure by the Russian government aimed at limiting the ability of foreign governments to evaluate public opinion in Russia and thus inhibiting their information warfare strategies.[397]

In November of 2017, the Russian State Duma unanimously passed a law labeling all media outlets that receive any funding from foreign citizens as “foreign agents.”[398] Such media outlets would be required to conduct a quarterly financial audit and provide the Russian authorities with detailed reports on all received and spent funds. Further, the affected media would also have to label all of their content as created by an entity, “performing the functions of a foreign agent.”[399] By the end of 2017, such media outlets

[394] “Putin podpisal zakon o zaprete mata v kino, spektaklyah I na koncertah [Putin signed a law banning obscenities in movies, performances and concerts].” TASS. May 5, 2014. Accessed July 31, 2022. https://tass.ru/kultura/1166943

[395] “V.Putin utverdil ‘smertnuyu kazn’’ dlya SMI [V. Putin approved the ‘death penalty’ for the media].” *RBC.ru* April 8, 2013. Accessed July 31, 2022. https://www.rbc.ru/politics/08/04/2013/570406559a7947fcbd4478e1

[396] “Putin zapretil innostrannym kompaniyam issledovat’ teleauditoriyu v Rossii [Putin bans foreign companies from researching TV audiences in Russia].” *RBC.ru.* July 4, 2016. Accessed July 31, 2022. https://www.rbc.ru/rbcfreenews/577a600e9a79471a6eb409f7

[397] For instance, Kier Giles characterizes such target audience analysis as “a critical enabler of information warfare,” which the Russian government viewed as a security vulnerability. See: Giles, “Handbook…”

[398] “Gosduma prinyala zakon o priznanii zarubezhnyh CMI inoagentami [The State Duma adopted a law on the recognition of foreign media as foreign agents].” *The BBC*. November 15, 2017. Accessed July 31, 2022. https://www.bbc.com/russian/news-41994050

[399] “Zakon o SMI-‘inoagentah’ nabiraet silu. Hronologiya [The law on media-‘foreign agents’ is gaining force. A chronology].” *OVD-Info.org*. June 21, 2021. Accessed July 31, 2022. https://ovdinfo.org/articles/2021/06/21/zakon-o-smi-inoagentah-nabiraet-silu-hronologiya

as *Voice of America, Radio Liberty,* TV channel *The Current Time*, were added to the "foreign agents" list.

In the following years, the Kremlin continued to purge the Russian media from foreign capital. Moreover, in 2021, Putin signed a law providing for up to five years in prison for individuals who are "foreign agents" for "malicious evasion" of their duties.[400] By the end of 2021, the number of "foreign agents" expanded to include more than one hundred media outlets, individuals, and NGOs.[401] As a result of this crackdown on independent media, in the 2021 World Press Freedom Index, compiled annually by international non-profit Reporters Without Borders, Russia sank to 150th place among the 180 rated countries.[402]

Table 2. Russia's ratings in the World Press Freedom Index 2011-2021

Russia's ratings in the World Press Freedom Index		
Year	**Russia's rating (lower is better)**	**Number of countries rated**
2011-2012	142	176
2013	148	179
2014	152	180
2015	152	180
2016	148	180
2017	148	180
2018	148	180
2019	149	180
2020	149	180
2021	150	180

[400] See *BBC*, "The number of media-"foreign agents" in Russia…"
[401] Yana Lomakina. "Kogo I za chto rossiyskiye vlasti vkluchili v reestr SMI-inostrannyh agentov – spisok Minjusta (obnovlyaemyi) [Whom and why did the Russian authorities include in the register of media-foreign agents - the list of the Ministry of Justice (updated)]." *TJournal.ru.* July 16, 2021. Accessed February 6, 2023. https://tjournal.ru/analysis/410978-kogo-i-za-chto-rossiyskie-vlasti-vklyuchili-v-reestr-smi-inostrannyh-agentov-spisok-minyusta-obnovlyaemyy; also, see "Chislo SMI-'inoagentov' v Rossii prevysilo 100 [The number of media-'foreign agents' in Russia exceeded 100]." *The BBC*. December 3, 2021. Accessed February 6, 2023. https://www.bbc.com/russian/news-59011912
[402] World Press Freedom Index. Reporters without Borders. Accessed July 31, 2022. https://rsf.org/en/index?year=2015

Overall, the Russian government's strategic campaign to curtail undesirable media led to a drastic change in its domestic information environment. If in 2011, the government registered nearly 7,000 new media outlets, in 2020, the number of registrations fell by more than 50 percent – to just over 3,000.[403]

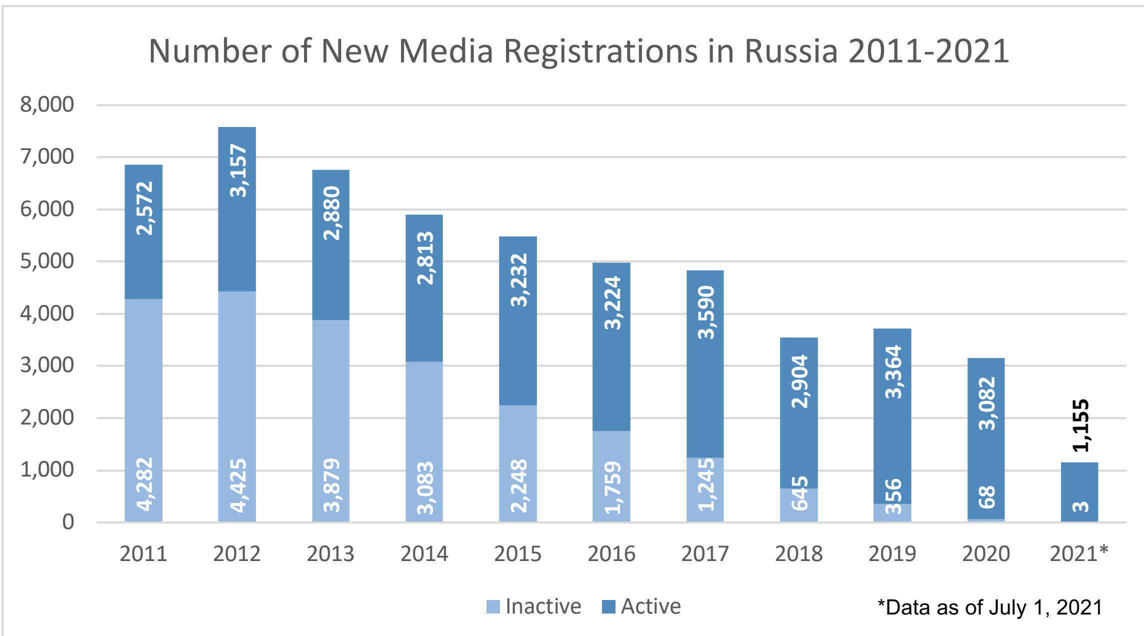

Figure 5. Number of new media registrations in Russia 2011-2021

At the same time, the number of government-owned Russian media continued to grow. For example, less than 10 percent of all media outlets registered in Russia in 2011 were government-owned. By 2020, that number rose to more than 26 percent.[404] However, even the non-government-owned media remain largely controlled by the Kremlin.

[403] Dada Lindell and Nikolai Yaroshenko. "SMI ne nuzhny. Za vosem let chislo vydavaemyh RKN licenziy sokratilos bolee chem v dva raza. Issledovanie 'MBH Media' [The media are not needed. Over eight years, the number of licenses issued by the RKN has more than halved. MBH media research.]." *MBK News*. July 9, 2021. Accessed July 31, 2022. https://mbk-news.appspot.com/sences/smi-ne-nuzhny/
[404] Lindell and Yaroshenko. "The media are not needed…"

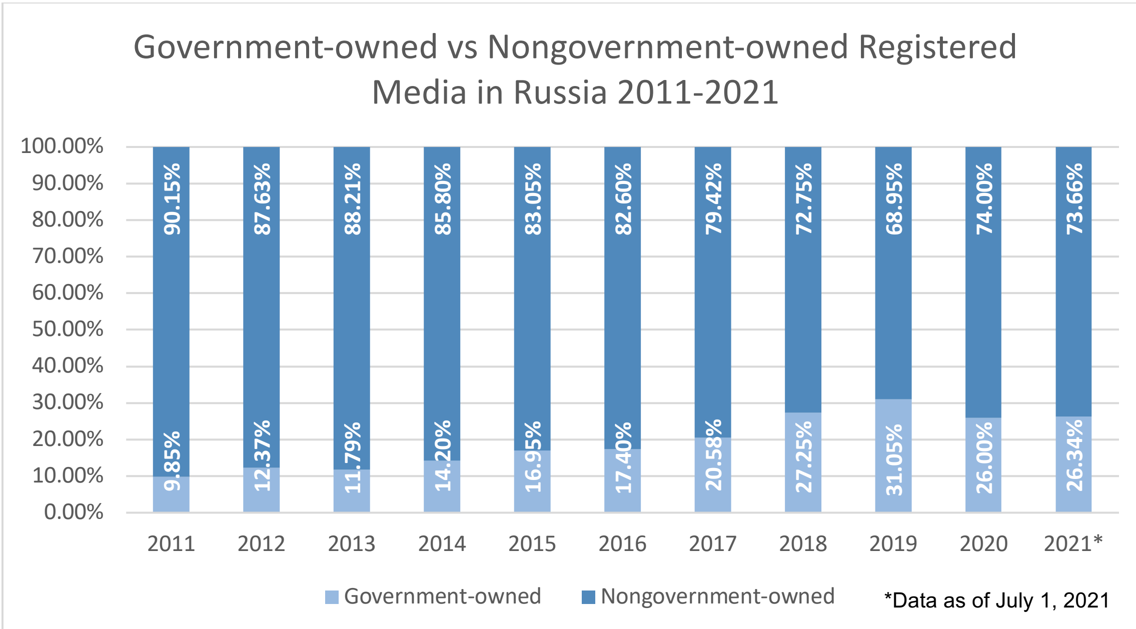

Figure 6. Government-owned vs. nongovernment-owned registered media in Russia 2011-2021

J. Protecting Russian Citizens from Foreign Information Influence

In my proposition "J," I posit that the Russian government would take further legal-administrative measures to protect Russian citizens from foreign information influence. This section tests this proposition by reviewing the government's observable actions directed at oversight and control of the Russian internet industry.

Russia has made impressive progress in the development of its IT infrastructure in the research period. The government spent trillions of rubles to bring its IT infrastructure into the twenty-first century, upgrading its IT systems, expanding broadband internet access, and funding a variety of high-tech startups. As a result, the Russian population has received faster, cheaper, and more readily available access to the internet.

At the start of 2011, only 50 million Russians (or 43 percent of the population) accessed the web on a regular basis. By 2021, the number of internet users more than doubled, growing to 124 million (or 85 percent of the population), with more than 3,000 telecom operators offering internet access services in the country as of that year.[405] The average internet speed in Russia increased from 6,4 Mbps in 2011, to 96.15 Mbps in 2021.[406]

As the number of Russian internet users grew, cyberspace emerged as a viable competitor to broadcast television, both in advertising budgets and audience size. According to the Levada Center, a Russian independent, nongovernmental polling and sociological research organization, in the 2011-2016 period, the internet replaced television as the main source of news among young Russians in the 18-24 age group.[407] By 2018, Runet's advertising revenue rose to 203 billion rubles ($3.2 billion in 2018), compared to 187 billion rubles ($2.9 billion) earned by television.[408] While television was still the main source of information for most Russians in 2021, its influence was on the

---

405 For 2010-2011 data, see: Lebedev, P.A. et al. "Internet v Rossii: Sostoyanie, tendencii i perspektivy razvitiya [Internet in Russia: current state, tendencies and development prospects]." Federalnoye agenstvo po pechati i massovym kommunikacyam. Upravlenie teleradiovewaniya i sredstv massovyh kommunikacyi [Federal Agency of Press and Mass Communications. Directorate of Broadcasting and Mass Communications]. 2011. ISBN 978-5-904427-15-3. Accessed July 31, 2022. https://raec.ru/activity/analytics/10122/; for 2021 data, see: "Chislo pol'zovateley interneta v Rossii dostiglo 124 mln [The number of Internet users in Russia reached 124 million]." TASS. October 19, 2021. Accessed March 7, 2023. https://tass.ru/obschestvo/12698757

406 For 2011 data, see: "Razvitie interneta v regionah Rossii [Internet access in the regions of Russia]." Yandex. 2012. Accessed July 31, 2022). https://yandex.ru/company/researches/2012/internet_regions_2012; for 2021 data, see: "2022 vs 2021 – UK Broadband and Mobile Speeds vs the World." *ISPreview.* December 29, 2022. Accessed March 7, 2023. https://www.ispreview.co.uk/index.php/2022/12/2022-vs-2021-uk-broadband-and-mobile-speeds-vs-the-world.html

407 Denis Volkov and Stepan Goncharov. "Rossiyskiy Media Landshaft – 2017 [Russian Media Landscape – 2017]." Levada-Centr [Levada Center]. August 22, 2017. Accessed March 7, 2023. https://www.levada.ru/2017/08/22/16440/

408 Istomina, Maria. "Reklama v internete vpervye obognala TV [Online advertising overtakes TV for the first time]." *RBC.ru.* March 11, 2019. Accessed July 31, 2022. https://www.rbc.ru/technology_and_media/11/03/2019/5c8619ce9a79473741c1055f

decline. Over the five years between 2017 and 2021, the share of Russians using TV as their news source decreased from 90 to 62 percent.[409] Instead, Russian citizens increasingly turned to websites like YouTube for their entertainment needs, while social media messengers like Telegram became the preferred sources of receiving and sharing daily news. For example, if in 2016, only a third of Russians used messaging apps, by 2021, three-quarters of Russians were regularly using them.[410] Recognizing this trend, the Kremlin began to increase its oversight of the internet industry, restricting it with new laws and eventually turning the Runet into the least free cyberspace in Europe.

One of the first domestic threats to Vladimir Putin's regime that emerged from cyberspace came in 2011 when large-scale civil protests erupted following a parliamentary election.[411] A massive crowd of 100,000 people, including anti-Putin opposition groups and regular citizens gathered on Moscow's Bolotnaya Square on December 10 to protest the election results. Social media played a big part in the protests as people used Facebook, Twitter, and VKontakte (the Russian version of Facebook) to organize and fund their efforts, which resulted in one of the biggest outbreaks of political dissent in Russia since the 1990s. Ever since then, Moscow's attempts to control the internet began to intensify.

Less than six months after the protests on Bolotnaya Square, President Putin signed Federal Law No.89417-6 titled "On the Protection of Children from Information Harmful to Their Health and Development." On paper, the law was meant to give the

---

[409] Denis Volkov et al. "Rossiyskiy Media Landshaft – 2021 [Russian Media Landscape – 2021]." Levada-Centr [Levada Center]. August 5, 2021. Accessed March 7, 2023. https://www.levada.ru/2021/08/05/rossijskij-medialandshaft-2021/
[410] Volkov, et al. "Russian Media Landscape – 2021"
[411] "Anatomiya sliva protesta. Kremlevskie eksperty vyyasnili, pochemu na mitingi hodit vse menshe ludei [Anatomy of a protest drain. Kremlin experts have found out why fewer people go to rallies]." *Lenta.ru.* December 6, 2012. Accessed July 31, 2022. https://lenta.ru/articles/2012/12/06/protest1/

government the ability to block content related to pornography, drug abuse, suicides, and even the denial of traditional family values.[412] However, in practice, the bill's vague language and no clear criteria for evaluating such online content essentially enabled Roskomnadzor to censor and block individual URLs and IP addresses. In just four months following the passage of the law, Roskomnadzor blocked around 4,000 websites.[413] As of this writing, the list of blocked sites includes more than 600,000 domains.[414]

By the end of 2013, as the Euromaidan protests in Ukraine continued to escalate, the Russian State Duma passed a law that allowed the government to block websites that contain extremist content or calls for participation in unsanctioned rallies.[415] The law was used to thwart public debate and silence voices that were critical of Russia's actions in Ukraine. For instance, on March 13, 2014, the Russian Prosecutor General's Office asked Roskomnadzor to block four major opposition websites that "contain calls for illegal activities and participation in mass events held in violation of the established order."[416] The websites included three news portals *Kasparov.ru* (founded by Russian chess

---

[412] Arina Borodina. "Televidenie stanet raznodostupnym [Television will become widely available]." *Kommersant.* August 23, 2012. Accessed July 31, 2022. https://www.kommersant.ru/doc/2006556

[413] "Monitoring Reyestra: Gosorgany udarno porabotali 23 fevralya (i +92 zaprewennyh IP [Registry Monitoring: State agencies worked hard on February 23 (and +92 banned IPs)]." *Roskomsvoboda.org.* February 27, 2013. Accessed July 31, 2022. https://roskomsvoboda.org/4445/

[414] "Reyestr zaprewennyh saitov [Registry of banned websites]." *Roskomsvoboda.org*. Accessed July 31, 2022. https://reestr.rublacklist.net/

[415] Kevin Rothrock. "Russia's Government Might Block Websites for Calls to Unsanctioned Rallies." GlobalVoices.org. December 15, 2013. Accessed July 31, 2022. https://globalvoices.org/2013/12/15/russias-government-might-block-websites-for-calls-to-unsanctioned-rallies/

[416] "Ogranichen dustup k ryadu internet-resursov, rasprostranyavshih prizyvy k nesankcionirovannym massovym meropriyatiyam [Access to a number of Internet resources that disseminated calls for unauthorized mass events was restricted]." Roskomnadzor. March 13, 2014. Accessed July 31, 2022. http://rkn.gov.ru/news/rsoc/news24447.htm

grandmaster Garry Kasparov), *Grani.ru, and EJ.ru,* as well as a personal blog page of Russian opposition leader Alexei Navalny (navalny.livejournal.com).

In sum, however, it could be said that the Kremlin largely kept its promise to "suppress the activity detrimental to the national security" by isolating Russia's population from information that does not fall in line with the government's point of view.[417] Although it is still possible for people living in Russia to access Western media and hear dissenting voices, all the traditionally trusted TV and radio platforms in the domestic information environment have been largely brought under the government's control. This means that the average Russian citizen now lives under an invisible Iron Curtain. While the majority of Russians are free to travel outside the country, their worldviews are now being actively shaped by an elaborate combination of information-technical and information-psychological tactics developed and perfected by the Russian government over many decades. As British writer and expert on Russian security issues, Kier Giles points out, "the result is broad acceptance of the alternative reality provided by state media, and a resultant state of collective delusion, voluntary or otherwise, among ordinary Russians."[418]

K. Developing National System of Russian Internet Segment Management

It follows from my proposition "K" that the Russian government would act to protect Russia's information space sovereignty by developing a national system of Russian internet segment management. I test this proposition in this section by investigating whether the Russian government took any significant steps in this regard.

[417] *Doctrine of Information Security…* Article IV, Section 23, Clause b).
[418] Giles, "Russia's 'New' Tools…"

To make it easier to identify dissenting voices in the Russian online information space, the Kremlin continued to introduce laws that allowed the government to gather personal information about Russian internet users. In August 2014, the government passed legislation requiring state-funded internet providers to verify people's identities before allowing them access to public Wi-Fi.[419] Later, in 2017, Putin signed another law further tightening control over the sales of SIM cards. The law obliges mobile operators to provide services only to individuals and legal entities whose personally identifiable information has been verified and entered into the database of the operators' payment systems.[420] As a result, for Russian users, access to the internet, either via public, household, or mobile access points, became largely tied to a person's physical identity.

In addition to restricting anonymous access to the internet, the Russian government also took steps to limit anonymous content. In August 2014, another law came into force in Russia, targeting independent bloggers.[421] According to the new legislation, bloggers with a daily audience of more than 3,000 visitors must register themselves as "mass media" with Roskomnadzor. The mass media status essentially requires hundreds of thousands of Russian bloggers to publish their legal name and contact information on their sites, list age restrictions for their content and holds them liable for publishing any content that could be deemed inaccurate, extremist, or as revealing of the private life of another citizen.

---

[419] Vladislav Mescheryakov. "Pred'yavlyat pasport dlya dostupa k Wi-Fi v parkah i kafe ne potrebuetsya [You won't need to show your passport to access Wi-Fi in parks and cafes]." *C-News.* August 8, 2014. Accessed July 31, 2022. https://safe.cnews.ru/news/top/predyavlyat_pasport_dlya_dostupa_k_wifi
[420] Albert Habibrahimov. "Putin podpisal zakon ob uzhestochenii kontrolya za SIM-kartami [Putin signed a law on tightening control over SIM-cards]." *VC.ru*. July 31, 2017. Accessed July 31, 2022. https://vc.ru/flood/25550-putin-sim
[421] "Bolee 130 blogerov, priravnennyh k SMI, zaregistriroval Roskomnadzor [Roskomnadzor has registered more than 130 bloggers equated with mass media]." *RIA Novosti* [*RIA News*]. November 11, 2014. Accessed July 31, 2022. https://ria.ru/20141111/1032859288.html

To help Roskomnadzor identify and block such large numbers of websites containing undesirable content, the government invested 84,2 million rubles ($1,26 million in 2016) in the development of a software-hardware site-monitoring system called “Revizor” (“Inspector”).[422] Beginning on December 1, 2016, Roskomnadzor mandated all Russian internet providers install the Revizor on their servers. If the system detects that the operator provides access to more than one percent of the blacklisted sites, it immediately notifies Roskomnadzor. The agency then orders the operator to restrict access to the identified sites within 24 hours.

To further support the government’s technical ability to enforce these policies, the Russian parliament passed a series of "anti-terrorist" amendments to several federal laws requiring internet providers to store all internet traffic on their servers for six months and all metadata for three years.[423] Additionally, all stored data, including people’s text messages, phone calls, and location data were to be turned over to authorities upon request.[424] This requirement followed another law implemented a year earlier in 2015, mandating data localization.[425] According to that law, all e-mail services, social networks, and search engines operating in Russia must store their data pertaining to Russian users on Russian territory. In November 2016, for failure to comply with this

---

[422] Anna Balashova, Dada Lindell, and Maria Kolomychenko. “Setevoy ‘Revizor’: kak rabotaet sistema kontrolya za zaprewennym kontentom [Network "Inspector": how the control system for prohibited content works].” *RBC.ru.* September 7, 2017. Accessed July 31, 2022. https://www.rbc.ru/technology_and_media/07/09/2017/59b00e269a79475c24ccf090

[423] Adam Maida. “Onlain I po vsem frontam. Nastuplenie na svobodu vyrazheniya mneniy v Rossii [Online and on all fronts. Attack on freedom of expression in Russia].” Human Rights Watch. July 18, 2017. Accessed July 31, 2022. https://www.hrw.org/ru/report/2017/07/18/306656

[424] Aleksandr Borzenko. “‘Paket Yarovoy’ prinyat bolshe polugoda nazad. Kak on rabotaet? [‘The Yarovaya Package’ was adopted more than six months ago. How does he work?].” *Meduza.io.* February 13, 2017. Accessed July 31, 2022. https://meduza.io/feature/2017/02/13/zakon-yarovoy-prinyat-bolshe-polugoda-nazad-kak-on-rabotaet

[425] Maida, “Online and on all fronts…”

requirement, the Russian government blocked the LinkedIn social network from operating in the Russian segment of the internet.[426] In sum, this series of restrictive laws enabled authorities to spy on and identify all Russian citizens without a court order, making any dissent, even online, an increasingly risky proposition.

At the same time, the Kremlin took a number of steps to defend its cyberspace from foreign influence. With a combination of legal and technical means, the government tried to make the Runet independent from the global internet, thus establishing its information space sovereignty. On November 1, 2019, a law on "ensuring the safe and sustainable functioning" of the internet went into effect in Russia.[427] Meant to protect the Runet from attacks or disconnection attempts from abroad, the legislation put Roskomnadzor in charge of controlling and routing all internet traffic within Russia.

To keep as much data as possible within Russian borders, the Federal Security Service created a special register of traffic exchange points between Russian and global networks. All Russian internet providers had to register their exchange points with the government and meet the requirements established by the FSB. Additionally, large service providers were required to take part in government exercises temporarily disconnecting the Runet from the global internet.[428] Such exercises have been conducted in both 2019 and 2021 (in 2020, exercises were canceled due to the global coronavirus pandemic) in coordination with the FSB, Ministry of Defense, Federal Protective Service

---

426 Maida, "Online and on all fronts…"

427 "Putin podpisal zakon o 'suverennom internete.' On vstupit v silu cherez polgoda [Putin signed the law on the 'sovereign Internet.' It will come into effect in six months.]." *The BBC*. May 1, 2019. Accessed July 31, 2022. https://www.bbc.com/russian/news-48126218

428 See *BBC,* "Putin signed the law on the 'sovereign Internet'…"

(FSO), Ministry of Emergency Situations, and Federal Service for Technical and Export Control.[429]

As part of the new system, Russian internet providers also had to install new equipment allowing Roskomnadzor to block undesirable websites more effectively using the DPI or the deep packet inspection method. Previously, the authorities relied primarily on IP addresses for blocking blacklisted sites. However, that method was largely ineffective as websites could easily bypass the block by simply changing their IP address.[430] "The era of a primitive understanding of the internet, which exists separately from the rest of society, is ending," noted Dmitry Peskov who serves as Vladimir Putin's Special Representative for Digital and Technological Development. "Everyone understands that as the internet grows into our lives, when it reaches the household, when it controls the light in our homes, energy and everything else, it cannot exist separately from state institutions. This is not a Russian situation, this is a global situation."[431] As a result of these efforts to control its domestic digital information space, by 2021, Russia topped the list of European countries with the least internet freedom, according to the non-governmental organization Freedom House.[432]

L. Increasing Cooperation on Information Security Issues with Regional Partners

[429] Darya Chebakova and Anna Balashova. "V Rossii protestirovali rabotu Runeta pri otkluchenii ot globalnoy Seti. Okonchatelnye itogi budut podvedeny cherez mesyac, seychas dannyh o sboyah net [In Russia, the operation of the Runet when disconnected from the global network was tested. Final results will be summed up in a month, currently there are no data on failures]." *RBC.ru*. July 21, 2021. Accessed July 31, 2022. https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739
[430] Chebakova and Balashova, "In Russia, the operation of the Runet…"
[431] "Eksperty rasskazali o posledstviyah zakona ob ustoichivom Runete [Experts spoke about the consequences of the law on resilient Runet]." *RIA Novosti* [*RIA News*]. November 1, 2019. Accessed July 31, 2022. https://ria.ru/20191101/1560469853.html
[432] Freedom on the Net 2021: Russia. FreedomHouse.org. Accessed July 31, 2022. https://freedomhouse.org/country/russia/freedom-net/2021

My proposition "L" is that Russia would use the political means of diplomacy to advance its InfoSec interests by increasing cooperation on InfoSec issues with member states of the CSTO, CIS, and SCO. This was also one of the central policy propositions stated in Russia's 2011 *Armed Forces' Information Space Activities Concept*. While researching Russia's observable actions in this regard, I found that, since 2011, Moscow has indeed notably increased its international cooperation efforts in the sphere of information security. For instance, in April 2011, Medvedev, along with presidents of China, Brazil, India, and South Africa (BRICS), issued a joint declaration at the conclusion of their summit in Sanya (China). The declaration became the BRICS' first document acknowledging the need to ensure international information security (IIS) and to fight cybercrime.[433]

The BRICS approach to InfoSec and cybercrime was then spelled out in greater detail in the 2014 Fortaleza Declaration adopted at this organization's summit in Brazil.[434] In 2015, BRICS leaders adopted another declaration during their summit in the Russian city of Ufa. The 2015 Ufa Declaration reinforced the member-states' verbal commitment to "territorial integrity and sovereign equality of states, non-interference in internal affairs of other state."[435] It also condemned "mass electronic surveillance and data collection of individuals all over the world" even though it was something that authoritarian members of BRICS, such as China and Russia, had already begun to engage in. This was also the first BRICS declaration featuring a list of specific areas of

---

[433] *Sanya Declaration*. BRICS Leaders Meeting, Sanya, Hainan, China, April 14, 2011. Accessed January 1, 2023. http://in.china-embassy.gov.cn/eng/xwfw/xxfb/201104/t20110415_2373458.htm
[434] *Fortaleza Declaration*. BRICS Leaders Meeting, Fortaleza, Brazil, July 15, 2014. Accessed January 1, 2023. http://www.brics.utoronto.ca/docs/140715-leaders.html
[435] *Ufa Declaration*. BRICS Leaders Meeting, Ufa, the Russian Federation, July 9, 2015. Accessed January 1, 2023. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/201507/t20150717_679402.html

cooperation in the sphere of IIS, such as coordinating efforts against cybercrime and working together to respond to computer security incidents, sharing best practices and information on IT security, and developing international norms and standards.

The Declaration of Brasilia, adopted at the BRICS summit in Brazil in 2019, similarly emphasized the need for cooperation on InfoSec and responsible conduct in cyberspace. It also underscored the importance of UN-recognized norms, rules, and principles in the area of ICTs.[436] Chaired by President Putin, the 2020 BRICS summit had originally been scheduled to take place in Saint Petersburg, Russia, but was instead held virtually due to the global COVID-19 pandemic. The Moscow Declaration welcomed the establishment of the BRICS Rapid Information Security Channel (BRISC), enabling the member states' central banks to exchange information on cyber threats.[437] It also expressed concern over the rising level of criminal misuse of ICTs and underscored the importance of establishing legal frameworks of intra-BRICS cooperation on ensuring security in the use of ICTs. The BRICS leaders restated similar concerns and intentions at the 2021 BRICS summit, held in India's capital of New Delhi.[438]

Besides signing a series of IIS agreements with the BRICS members, Russia has signed similar deals with members of the CSTO, CIS, and SCO, as well as several non-member states, such as the Philippines, Vietnam, South Africa, and Cuba. In 2013,

---

[436] *Brasilia Declaration*. BRICS Leaders Meeting, Brasilía, Brazil, November 14, 2019. Accessed January 1, 2023. http://www.brics.utoronto.ca/docs/191114-brasilia.html

[437] Earlier that year, Russia also chaired several InfoSec-related meetings, including BRICS Working Group on ICT and High-Performance Computing; BRICS Working Group on Security in the Use of ICTs; and BRICS Working Group on ICT Cooperation. For more details, see *Moscow Declaration*. BRICS Leaders Meeting, Moscow, the Russian Federation, November 17, 2020. Accessed February 27, 2023. http://www.brics.utoronto.ca/docs/201117-moscow-declaration.html

[438] *New Delhi Declaration*. BRICS Leaders Meeting, New Delhi, India, September 9, 2021. Accessed February 27, 2023. http://www.brics.utoronto.ca/docs/210909-New-Delhi-Declaration.html

Russia signed an agreement with Belarus, a member of both the CIS and the CSTO.[439] The agreement called for cooperation on the provision of information and communication security for national critical infrastructure. In 2014, Russia signed a bilateral agreement "On cooperation in the field of IIS support" with the Republic of Cuba.[440] In 2017, a similar agreement was signed with the Republic of South Africa.[441] Both agreements called for the creation of a joint system for monitoring and responding to information threats and cooperation in investigating cases of the use of ICTs for criminal purposes, training InfoSec experts, and advancing the relevant norms of international law.

Also in 2017, Russia signed a multilateral agreement on InfoSec with members of the CSTO.[442] The agreement expressed the governments' concerns with the increasing number of threats coming from the information space and underscored their commitment to preventing the use of IT for the purpose of destabilizing situations in their countries or damaging critical infrastructure. Additionally, the agreements defined the assurance of information security as a priority area of ensuring collective security among member states.

---

439 "Belarus, Russia to expand cooperation in information security." *Belta.* September 10, 2019. Accessed January 15, 2023. https://eng.belta.by/politics/view/belarus-russia-to-expand-cooperation-in-information-security-124031-2019/

440 "Soglashenie mezhdu Pravitel'stvom Rossiyskoy Federacii i Pravitel'stvom Respubliki Kuba o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informacionnoy bezopasnosti [Agreement between the Government of the Russian Federation and the Government of the Republic of Cuba on cooperation in providing international information security]." The Ministry of Foreign Affairs of the Russian Federation. July 11, 2014. Accessed January 15, 2023. http://publication.pravo.gov.ru/Document/View/0001201501140003?rangeSize=20

441 "Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security." The Ministry of Foreign Affairs of the Russian Federation. September 4, 2017. Accessed January 15, 2023. https://archive.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2854430

442 "Soglashenie o otrudnichestve gosudarstv – chlenov Organizacii Dogovora o kollektivnoy bezopasnosti v oblasti obespecheniya informacionnoy bezopasnosti [Agreement on cooperation between the member states of the Collective Security Treaty Organization in the field of ensuring information security]." The Ministry of Foreign Affairs of the Russian Federation. November 30, 2017. Accessed January 15, 2023. http://publication.pravo.gov.ru/Document/View/0001201904260001

Bilateral agreements with the Republic of Vietnam and the CIS member Turkmenistan were signed in 2018 and 2019 respectively.[443] Both documents affirmed the parties' alignment in their assessments of information and computer threats and called for closer cooperation on IIS issues. All of these agreements are very similar in their language and lack substantive action steps or timebound objectives. However, they present the Russian government with opportunities to further cultivate relationships with other countries, develop deeper cooperation on IIS issues, and build a Russia-led coalition of like-minded states in order to shift the Western narrative on the established internet governance.

M. Shaping and Defining Norms of International Information Security under Auspices of United Nations

According to my proposition "M," to advance its stated InfoSec strategy in 2011-2021, the Russian government would aim to conclude an IIS treaty under the auspices of the UN and continue to advocate more international internet governance. This section tests the validity of this proposition by examining the record of Russia's InfoSec initiatives in the UN in the research period.

[443] "Soglashenie mezhdu Pravitel'stvom Rossiyskoy Federacii i Pravitel'stvom Socialisticheskoy Respubliki V'etnam o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informacionnoy bezopasnosti [Agreement between the Government of the Russian Federation and the Government of the Socialist Republic of Vietnam on cooperation in the field of ensuring international information security]." The Ministry of Foreign Affairs of the Russian Federation. September 6, 2018. Accessed January 15, 2023. http://publication.pravo.gov.ru/Document/View/0001201904290008?index=5&rangeSize=1; also see "Soglashenie mezhdu Pravitel'stvom Rossiyskoy Federacii i Pravitel'stvom Turkmenistana o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informacionnoy bezopasnosti [Agreement between the Government of the Russian Federation and Turkmenistan on cooperation in providing international information security]." The Ministry of Foreign Affairs of the Russian Federation. April 5, 2019. Accessed January 15, 2023. http://publication.pravo.gov.ru/Document/View/0001201906130020?index=2&rangeSize=1

Global cybersecurity regulations have been a major focus for Russia even before the publication of the major strategic doctrines reviewed in this thesis. For Moscow, the established internet governance represents a unipolar world order led by the U.S. Therefore, contesting it goes hand-in-hand with Russia's strategic quest for regaining its historic role as a great power.

Russia has promoted its vision of IIS since the late 1990s when it introduced its first draft resolution on ICT in the UN General Assembly.[444] At that time, Russian officials managed to convince the First Committee that ICTs could be used by terrorist, extremist, or criminal groups "for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States."[445] Almost every year since 1998, Russia has tabled resolutions at the UN that aimed to prohibit the use of ICTs in ways that may negatively impact the security or regime stability of sovereign states. While these efforts have not always been successful at establishing new norms, the Kremlin has managed to grow its pool of sympathetic countries that regularly co-sponsor its diplomatic initiatives.

Russia's contestation over global internet governance in recent years reflects its overall vision of a new more equitable international order expressed in its doctrinal documents. In 2011, the Russian delegation, along with the delegations of China, Tajikistan, and Uzbekistan (all members of the SCO) submitted a proposal for an *International Code of Conduct for Information Security* (*the Code*) to the UN General

---

[444] Xymena Kurowska. "What does Russia want in cyber diplomacy? A primer." Central European University. EU Cyber Direct Research Paper. December 2019. Accessed July 31, 2022. https://www.ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf
[445] Elaine Korzak. "Russia's Cyber Policy Efforts in the United Nations." NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Tallinn Paper No.11 2021. Accessed July 31, 2022. https://www.ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf

Assembly.[446] *The Code* stressed the respect for state sovereignty and called for the non-proliferation of information weapons. Among its eleven voluntary commitments, the document urged states to cooperate in "curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[447] *The Code* also promoted "the establishment of a multilateral, transparent and democratic international Internet management system."[448]

Currently, global internet governance relies on the *Budapest Convention on Cybercrime*, an international treaty adopted by the Council of Europe on November 8, 2001, and opened for signature on November 23, 2001, in Budapest, Hungary.[449] Ratified by sixty-six states, the Convention established a framework of laws and procedures pertaining to crimes committed in cyberspace.[450] Russia did not join *the Budapest Convention* and has been categorically opposed to some of its provisions, such as the 32nd article allowing cross-border operations by intelligence agencies without notifying national authorities.[451] In Moscow's view, such cross-border access comes in direct conflict with the principles of national sovereignty. After numerous unsuccessful attempts to convince the Council of Europe to amend the 32nd article of *the Budapest Convention*, the Kremlin began agitating for a new treaty to replace it altogether.

---

[446] "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." General Assembly of the United Nations. A/66/359. Accessed July 31, 2022. https://www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E
[447] See UN General Assembly "Letter dated 12 September 2011…"
[448] See UN General Assembly "Letter dated 12 September 2011…"
[449] Details of Treaty No.185, Council of Europe. Accessed July 31, 2022. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
[450] See Council of Europe, Parties/Observers to the Budapest Convention…
[451] Elena Chernenko. "Belorussiya vybrala internet pobezopasnee [Belarus chose a safer internet]." *Kommersant.* June 7, 2012. Accessed July 31, 2022. https://www.kommersant.ru/doc/1953059

In September 2011, Russia released a *Draft Convention on International Information Security.*[452] Meant to be binding at the international level, the Convention reflects the main issues of concern stated in Russia's doctrinal documents. For instance, some of the major ICT threats to international peace and security listed in the document include the following:

- Purposefully destructive behavior in the information space aimed against critically important structures of the government of another State
- The illegal use of the information resources of another government without the permission of that government, in the information space where those resources are located
- Actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilizing society
- The manipulation of the flow of information in the information space of other governments, disinformation, or the concealment of information to adversely affect the psychological or spiritual state of society, or erode traditional cultural, moral, ethical, and aesthetic values[453]

The disagreement over *the Budapest Convention* serves as a perfect illustration of the differences in the approaches toward internet governance between Russia and the West. While Russia insists that the concepts of a State's sovereignty apply to cyberspace, the U.S. and its Western allies treat it as a neutral domain.[454] While Russia aims to

[452] See *Russian Draft Convention on International Information Security.*
[453] See *Russian Draft Convention on International Information Security.*
[454] Pavel Sharikov. "Global Cybersecurity at Stake Amid US and Russia's Disagreements." Italian Institute for International Political Studies. September 7, 2021. Accessed July 31, 2022.

strengthen the power of the State over cyberspace in order to exercise stricter social control over it as a medium, the U.S. has adopted a philosophy that the internet as a technology is non-political, and the government's primary role is to ensure equal opportunities for those who use it.

The U.S. doesn't attempt to regulate the potential use of cyberspace for information-psychological warfare. According to the Western approach, international regulations directed at limiting such activities would inevitably come into conflict with the Universal Declaration of Human Rights, which guarantees everyone their right to freedom of opinion and expression.[455] From the standpoint of diplomacy, the U.S. approach to IIS focuses on law enforcement at the domestic level with voluntary international cooperation, while Russia focuses on establishing a binding system of international supervision.[456]

Ramping up its IIS diplomacy efforts, in March 2012, the Russian Ministry of Foreign Affairs created a new position of special coordinator on matters of the use of ICTs for political purposes.[457] Andrey Krutskikh, who previously worked as deputy director of the Ministry's Department of New Challenges and Threats, was appointed to the role. Krutskikh reportedly played a direct role in the development of both *the*

---

https://www.ispionline.it/en/pubblicazione/global-cybersecurity-stake-amid-us-and-russias-disagreements-31435

[455] Waseem Ahmad Qureshi. "Information Warfare, International Law, and the Changing Battlefield." *Fordham International Law Journal.* Vol. 43:4 (2020). Accessed July 31, 2022. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2786&context=ilj

[456] Franz-Stefan Gady and Greg Austin. "Russia, The United States, And Cyber Diplomacy: Opening the Doors." EastWest Institute. 2010. Accessed July 31, 2022. https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf

[457] Elena Chernenko. "V MIDe poyavilsya curator interneta [The Ministry of Foreign Affairs got an internet curator]." *Kommersant.* March 20, 2012. Accessed August 1, 2022. https://www.kommersant.ru/doc/1896438

International Code of Conduct for Information Security and *the Draft Convention on International Information Security*.[458]

In the following years, Russia has made considerable progress in advocating its vision of IIS, particularly, through its work in the Groups of Governmental Experts (GGEs) established by the UN General Assembly to study various aspects of IIS. Moscow's involvement in GGEs between 2012-2015 resulted in the establishment of the international normative framework for responsible state behavior in cyberspace.[459] The framework is comprised of eleven non-binding norms calling for the application of international law to the use of ICTs by states that results in intentional damage to critical infrastructure, as well as encouraging interstate cooperation with regards to malicious ICT activity while "taking into account due regard for sovereignty."[460]

In 2018, Russia successfully sponsored two resolutions, both of which can be viewed as significant accomplishments for Russian InfoSec diplomacy. The first resolution, titled *Countering the use of information and communications technologies for criminal purposes,* aimed to start an alternative discussion on IIS with the goal of developing a replacement for *the Budapest Convention*.[461] The second resolution, titled *Developments in the field of information and telecommunications in the context of international security,* offered its own version of the norms of responsible state behavior established by the 2013-2015 GGEs, expanding them from the eleven outlined in the

---

[458] Chernenko, "The Ministry of Foreign Affairs got an internet curator."
[459] Korzak, "Russia's Cyber Policy Efforts…"
[460] Bart Hogeveen. "The UN norms of responsible state behaviour in cyberspace." Australian Strategic Policy Institute (ASPI), International Cyber Policy Centre. March 22, 2022. Accessed August 1, 2022. https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace
[461] "Countering the use of information and communications technologies for criminal purposes." General Assembly of the United Nations. A/RES/73/187. 2018. New York. Accessed August 1, 2022. https://digitallibrary.un.org/record/1660536?ln=en

U.S.-sponsored resolution to thirteen.[462] It also called for the establishment of an open-ended ad hoc intergovernmental committee of experts that would be representative of all regions and deliberate on cybersecurity issues. In essence, these open-ended working groups (OEWGs) were meant to serve as a more inclusive alternative to GGEs that were limited to no more than twenty-five member states. By expanding the pool of participating states, Russia hoped to broaden its coalition with countries that tend to share its interpretation of IIS, including the CIS members, as well as several states across Asia, Africa, and Latin America.

In response, the U.S. and its co-sponsors submitted a competing resolution titled *Advancing responsible State behaviour in cyberspace in the context of international security*.[463] The document urged states "to be guided in their use of ICTs by the 2010, 2013, and 2015 reports of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security."[464] Additionally, the resolution created a new GGE to study how international law applies to the use of ICTs by states. Although Russia and the U.S. positioned their respective resolutions as mutually exclusive, the UN General Assembly voted in favor of adopting both, which further complicated the international conversation on cyberspace.[465]

Continuing to pursue its objectives, Russia took the initiative once again in 2019 with a new resolution on cybercrime. The document proposed the creation of a new

---

462 "Developments in the field of information and telecommunications in the context of international security." General Assembly of the United Nations. A/C.1/73/L.27/Rev.1. October 29, 2018. New York. Accessed August 1, 2022. https://bit.ly/3S3Bg9R

463 "Advancing responsible State behaviour in cyberspace in the context of international security." General Assembly of the United Nations. A/C.1/73/L.37. Accessed August 1, 2022. October 18, 2018. https://bit.ly/3YDK74w

464 See UN General Assembly resolution "Advancing responsible State behaviour in cyberspace…"

465 Korzak, "Russia's Cyber Policy Efforts…"

OEWG "to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes."[466] Unsurprisingly, the initiative was met with strong opposition by the U.S. and its allies who perceived it as a direct attempt by both Russia and China to supplant *the Budapest Convention*. Critics argued that the vaguely worded document would enable states to arbitrarily designate online activities as cybercrime, which would then allow them to block websites at will and use cyberspace to crack down on political opposition:

> "The big picture is that Russia and China are seeking to establish a set of global norms that support their view of how the Internet and information should be controlled," an anonymous European official commented on the matter. "They're using every means they can in the U.N. and elsewhere to promote that. This is not about cybercrime. This is about who controls the Internet."[467]

Nevertheless, despite the strong pushback from a number of major Western powers and human rights groups, the Russian resolution was adopted with 88 votes in favor, 58 against, and 34 abstentions.[468]

In July of 2021, Russia submitted a draft of the *Convention on countering the use of information and communications technologies for criminal purposes* to the acting

---

466 "Countering the use of information and communications technologies for criminal purposes." General Assembly of the United Nations. A/C.3/74/L.11/Rev.1. November 5, 2019. Accessed August 1, 2022. https://undocs.org/A/C.3/72/12

467 Ellen Nakashima. "The U.S. is urging a no vote on a Russian-led U.N. resolution calling for a global cybercrime treaty." *The Washington Post*. November 16, 2019. Accessed August 1, 2022. https://wapo.st/3xr6yOr

468 An international coalition of human rights groups wrote a public letter to the General Assembly, strongly urging the delegation to vote against the resolution. For more information, see "Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online." Association for Progressive Communications. November 6, 2019. Accessed August 1, 2022. https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human. For more details on the UN vote, see "Report on the 74th session of the Third Committee of the UN General Assembly." Universal Rights Group. November 25, 2019. Accessed August 1, 2022. https://www.universal-rights.org/blog/report-on-the-74th-session-of-the-third-committee-of-the-un-general-assembly/

Director of the United Nations Office on Drugs and Crime Dennis Thatchaichawalit.[469] Just like Moscow's previous initiatives, the proposal aims to broaden the government's oversight over its cyberspace by significantly expanding the set of cyber offenses that the current international rules recognize. The new Convention calls on member states to develop domestic laws punishing the use of ICTs "for subversive or armed activities directed towards the violent overthrow of the regime of another state," and enabling them to "collect or record […] information transmitted by means of ICT," as well as obliging service providers to do the same.[470] The sixty-nine-page document also urges for increased international cooperation in tracing, arresting, and extraditing people suspected of cybercrimes.[471] According to the civil rights nonprofit the Electronic Frontier Foundation, "the treaty, if approved, may reshape criminal laws and bolster cross-border police surveillance powers to access and share user data, implicating the privacy and human rights of billions of people worldwide."[472]

In addition to submitting its Convention to the UN, the Russian delegation, led by Deputy Prosecutor General Pyotr Gorodovoy, handed a copy of the draft to the OEWG it had previously established with its resolution in 2019.[473] The intergovernmental group was tasked with elaborating the future international treaty on cybercrime. "Russia is the first country to elaborate and submit to the ad hoc committee a draft universal convention

[469] "Russia initiates its draft of int'l convention on countering cybercrime." TASS. July 27, 2021. Accessed August 1, 2022. https://tass.com/politics/1318319
[470] "Convention on countering the use of information and communications technologies for criminal purposes." General Assembly of the United Nations. Articles 19, 33. June 29, 2021. Accessed August 1, 2022. https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf
[471] See UN General Assembly, "Convention on countering…" Article 47.
[472] Katitza Rodriguez and Karen Gullo. "Negotiations Over UN Cybercrime Treaty Under Way in New York, With EFF and Partners Urging Focus on Human Rights." Electronic Frontier Foundation. March 3, 2022. Accessed August 1, 2022. https://www.eff.org/deeplinks/2022/03/negotiations-over-international-police-powers-agreement-must-keep-human-rights
[473] TASS, "Russia initiates its draft…"

on countering information crimes," stated the Russian prosecutor general's office in a press release. "Russia offers to the world its own ideas that could form the basis of a future comprehensive instrument, which will be developed with due account of the positions of other world nations."[474] Gorodovoy's words not only echo the proposition tested in this section, but they also underscore the consistent diplomatic effort to that end that Moscow demonstrated over the 2011-2021 period.

This chapter has tested the propositions about Russia's expected behavior, based on its stated information security strategy as outlined in Chapter II. The testing was done by correlating these propositions with observable actions of the Russian government in the 2011-2021 research period. While testing these propositions, this chapter illustrated how the Russian government aligned the *ends*, *ways,* and *means* of its InfoSec strategy.

Specifically, I found that, to defend against the perceived threat of the use of ITs to undermine Russia's sovereignty, political and regional stability, the State used such military *means* as General Staff's GRU and the defense ministry's information operations troops, EW troops, as well as special military units known as "scientific companies." The government used those means in *ways* that leveraged ITs in order to strengthen the capabilities of the Russian military and InfoSec services. To the same end, Russia used such external political *means* as diplomacy in *ways* that would help it shape and define norms of information security and global internet governance via international treaties.

I also found that, to counter the threat of Russia's dependence on foreign ITs, the Russian authorities used legal-administrative and economic *means* in the form of government policies and allocations from the federal budget in *ways* that were supposed

[474] TASS*,* "Russia initiates its draft…"

to help Russia develop domestic IT sectors. The Kremlin also employed available economic *means* in the form of various government subsidies in *ways* that promoted the Russian media in the global information space. This, in turn, was supposed to increase Russia's soft power, thus enabling the State to better address the perceived threat of biased assessments of Russian policy.

Addressing the perceived threats of discrimination of the Russian language and media abroad, as well as subversive information activities aimed at undermining traditional moral, spiritual, and patriotic values, the Russian State used its social-psychological *means* by *way* of leveraging the spheres of culture and education to expand the teaching of the Russian language abroad and instill traditional values in its citizens. Finally, to further "shield" the Russian citizens and society from subversive internal and external information influence, the Russian government employed its legal-administrative *means* in the form of restrictive laws and regulations aimed at establishing total control over the domestic information environment.

This broad examination of the Russian State's actions pertaining to the *ends, means,* and *ways* of its InfoSec strategy has yielded evidence that merits further investigation of whether my thesis' primary question can be given an affirmative answer. In the next chapter, I will compare Russia's words and actions to ascertain whether, indeed, the government's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain.

Chapter IV.

Russia's Information Security Strategy: Do Russia's Words and Actions Align?

In Chapter II, I examined the written *words* of the Russian government in the InfoSec domain by analyzing its strategic doctrines, outlining the essential elements of the Russian information security strategy, and advancing specific propositions regarding the country's expected behavior and resource allocation decisions in 2011-2021. In Chapter III, I examined the Russian government's *actions* in that domain by testing my propositions against Russia's observable behavior. I will now compare these words and actions with regard to the *ends, means,* and *ways* of Russia's InfoSec strategy in Chapter IV to attempt to answer my primary research question: *do Russia's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain?*

As described in Chapter II, Russia's stated InfoSec strategy in 2011-2021 was, to a significant extent, based on the Russian leaders' belief that their country was locked in a multi-domain confrontation with the West, including confrontation in the information domain. This confrontation, as well as the need to retain the Russian public's loyalty to the ruling regime, were the major reasons why the Russian State sought to attain such *ends* in its stated InfoSec strategy, as "shielding" its citizens, society, and itself from what it framed as internal and external information threats. Those perceived threats were as follows: use of ITs to undermine Russia's sovereignty, political and regional stability; discrimination of the Russian language and media abroad; biased assessments of Russian policy; Russia's dependence on foreign ITs; as well as subversive information activities aimed at undermining traditional moral, spiritual, and patriotic values.

To attain these "protective" *ends*, Russia's stated InfoSec strategy called for the employment of legal-administrative, political, economic, social-psychological, and military *means*, which I also outlined in Chapter II. The strategy prescribed six distinct *ways*, in which these *means* were to be employed to attain the aforementioned protective *ends*. Those included: (1) leveraging ITs to strengthen the capabilities of the Russian military and InfoSec services; (2) developing domestic IT sectors; (3) utilizing the spheres of culture and education; (4) growing the Russian soft power through the promotion of the Russian media in the global information space; (5) controlling the domestic information environment; and (6) shaping and defining norms of InfoSec and global internet governance via international treaties. Based on these stated *ends, means*, and *ways*, I advanced thirteen propositions regarding Russia's expected actions toward advancing its InfoSec strategy, as described in Chapter II.[475] Having tested those propositions in Chapter III, I found them to be aligned with my observations of the Russian State's behavior in the research period. The table below presents a summary of my findings. It is followed by a brief description of how the Russian State and its key agents implemented their strategy in reality.

Table 4. Comparing propositions regarding Russia's expected actions based on its stated information security strategy with observed behavior in 2011-2021

	Propositions regarding Russia's expected behavior and resource allocation decisions	**Were actions consistent with strategy?**
A.	The Russian government would work on enhancing its capacity and means of information warfare	Yes
B.	The Russian government would launch efforts to train new information space specialists	Yes

[475] As with the *ends, means*, and *ways* of Russia's stated InfoSec strategy, I derived my propositions about Russia's expected behavior from the InfoSec-related postulates that I could find in its doctrinal documents (as summarized in Table 1.)

C.	The Russian government would use the means of its military to develop an IT-based system for assessing and forecasting the military and political situations at global and regional levels	Yes
D.	The Russian government would use its legal-administrative and/or economic means to become less dependent on Western ITs	Yes
E.	The Russian government would invest in the scientific and high-tech industries to create advanced IT and InfoSec solutions, goods, and services for domestic and international markets	Yes
F.	The Russian government would promote traditional moral, spiritual, and patriotic values among its citizens, as well as the study of the Russian language abroad by using the social-psychological means of culture and education	Yes
G.	The Russian government would employ its economic means to create state-funded media and information resources to provide both domestic and international audiences with the Kremlin's point of view on Russian policies and world events	Yes
H.	The Russian government would work on developing its own effective means of information influence on public opinion abroad	Yes
I.	To prevent the use of ITs to undermine Russia's sovereignty, political and regional stability the Kremlin would use available legal-administrative means to establish better government control within its information sphere	Yes
J.	The Russian government would use available legal-administrative means to protect Russian citizens from foreign information influence	Yes
K.	To protect Russia's information space sovereignty, the government would work on developing a national system of the Russian internet segment management	Yes
L.	Russia would increase cooperation on information security issues with member states of the CSTO, CIS, and SCO	Yes
M.	The Russian government would aim to conclude an IIS treaty under the auspices of the UN and continue to advocate a more international internet governance	Yes

Consistent with my propositions, in the 2011-2021 period, the Russian government took a concerted effort to strengthen the capabilities of the Russian military and services responsible for information security. To attain the strategic *end* of protecting the Russian State, its citizens, and society from perceived internal and external information threats, the FSB created a new system for monitoring and responding to cyberattacks known as GosSOPKA. The Kremlin has transformed Roskomnadzor, a relatively unimportant regulatory agency before 2011, to a powerful information warfare machine with vast resources, political power, and technical capabilities.

Utilizing its military *means*, Russia significantly increased its EW capabilities, having procured a large number of new EW systems, and made EW troops an integral part of its military operations. The government even created an entirely new branch of the military – the Russian information operations troops – dedicated to combatting information threats and conducting disinformation and counterpropaganda activities. Russia also created new talent pipelines for the recruitment and training of skilled information space specialists. Finally, the Ministry of Defense created the National Defense Management Center to collect and analyze real-time data about military and political developments in Russia and abroad.

Acting in accordance with its stated InfoSec strategy, Russia utilized the available economic *means* to lessen the State's dependence on foreign ITs by *way* continually increasing budget allocations for the scientific and high-tech sectors. To accomplish this strategic *end*, the government allocated trillions of rubles to several federal programs aimed at the development of IT infrastructure, high technologies, and digitization of the federal government. Dedicated initiatives, such as the "Digital Economy" and "Education Development" programs, focused on educating new specialists to supply the Russian economy with highly qualified workforce in priority areas of modernization and technological development. Although many of these initiatives failed to achieve their desired ends, some, such as the government program "Information Society," produced significant measurable outcomes.

Russia also dedicated significant effort to increasing its information security by reducing the government's exposure to foreign ITs. Using its legal-administrative *means*, the Kremlin adopted new laws to limit government purchases of foreign software, developed initiatives to transition state-owned companies to domestic software, and repeatedly discussed switching to domestically produced communications equipment. Meanwhile, many Russian companies were able to expand their IT and InfoSec offerings abroad. Several government-affiliated companies even signed a number of contracts for providing cybersecurity services to foreign states.

In pursuit of its strategic *end* of defending Russian society against subversive information activities aimed at undermining traditional moral, spiritual, and patriotic values, the Kremlin employed the social-psychological *means* of culture. Between 2013 and 2020, the Russian government allocated billions of rubles to its "Culture Development" program aimed at developing a common civic identity and strengthening the unity of the Russian nation. As part of the program, the government produced and distributed patriotic content via multimedia channels and created numerous digital resources aimed at popularizing the Russian cultural heritage. In sum, the Kremlin invested billions in dollar equivalent to increase the presence of such content in the domestic media market.

Another *way* in which the government utilized the available social-psychological *means* was by leveraging the sphere of education to develop special digital programs aimed at instilling traditional moral values and patriotic attitudes in the younger generation of Russians. A dedicated subprogram focused on promoting the use and study of the Russian language abroad as a *way* to counter the perceived threat of language discrimination. The government also introduced new software and remote learning tools to make education in Russian more accessible to people living abroad.

In 2011-2021, the Russian State made a concerted effort to grow the Russian soft power by using economic *means* in *ways* that would promote the Russian media in the global information space. Doing so was supposed to help the government achieve the strategic *end* of defending Russia against the perceived discrimination of the Russian media and biased assessments of Russian policy abroad. As such, Moscow methodically allocated financial resources to support state-owned media outlets and was able to expand its media conglomerate internationally. Even as the Russian economy suffered from the economic sanctions following its incursion in Ukraine, the government continued to increase funding for Russian-language digital media. Russian news outlets, such as *RT, Sputnik, TASS,* and *RTR* all received massive government subsidies and were able to significantly grow both their domestic and international audiences.

Additionally, Russia was able to further enhance its IW capabilities by developing its own effective means of information influence on public opinion abroad. It did so by allocating economic resources to create a massive and complex network of computer bots, troll factories, and hackers to carry out both information-technical and information-psychological operations. This, in turn, enabled Moscow to manipulate the information environment, sowing discord in the West while consolidating public opinion at home.

In line with my propositions, the Russian authorities also took extensive actions to achieve the strategic *end* of defending the State against the potential use of IT to undermine Russia's sovereignty, political and regional stability. The government employed available legal-administrative *means* in ways that enabled it to control Russia's domestic information environment. Specifically, the Kremlin used a combination of restrictive laws, regulations, and technological implementations to monitor domestic media and severely restrict the freedom of information within the Russian segment of the internet. As a result, the government was able to curtail nearly all undesirable media within the country, thus isolating the Russian population from information that contradicts the Kremlin's point of view.

The Russian authorities also expended notable effort in making the Runet independent from the global internet. The government introduced legislation that forced all Russian internet providers to store all internet traffic data within Russian territory. The Russian Ministry of Defense along with the FSB and several other agencies also began to conduct annual exercises temporarily disconnecting the Runet from the global internet with the goal of making it more independent from the World Wide Web and more resilient to cyberattacks.

To further pursue the strategic *ends* of protecting its information space sovereignty, Russia used external political *means* in the form of diplomacy in *ways* that enabled it to shape and define norms of information security and global internet governance. Specifically, Moscow made considerable progress in utilizing international treaties to increase cooperation efforts on InfoSec within the regional groupings of the BRICS, CIS, SCO, and CSTO, as well as several individual states. While these agreements appeared superficial in their language, they allowed Russia to build its image as a reputable partner on matters of InfoSec and even expand its access to the information infrastructure of other states. Importantly, these agreements also allowed Russia to reinforce its narratives on internet sovereignty, expand its coalition in the UN, and position itself as an alternative to Western approaches to global internet governance.

Throughout the research period, the Kremlin methodically advanced its stated InfoSec strategy by attempting to redefine international cyber norms and advocate stricter cyberspace regulations across the UN system and beyond. In its proposals, Moscow, along with its allies, consistently tried to broaden the definitions of cybercrime, cyber weapons, and national sovereignty in cyberspace. Still, fundamental differences in the approaches toward InfoSec between Russia and the U.S. remain a significant obstacle to Moscow's cyber diplomacy efforts. Nevertheless, despite continued resistance from the U.S. and like-minded states, some of Russia's initiatives to replace the Budapest Convention with a new cybercrime treaty gained significant momentum. I should note, however, that, while some of Russia's InfoSec initiatives produced tangible results, many, such as the import-substitution of foreign software, fell short of the desired outcome. As is often the case with Russia, many of the government-funded programs reviewed in this study were bogged down by chronic corruption and inefficiencies of the Russian State.

As it follows from my comparison of Russia's words and actions in the InfoSec domain conducted above and summarized in Table 5 below, the Russian State's behavior in the InfoSec domain in 2011-2021 was consistent with the *ends, means*, and *ways* of its stated InfoSec strategy in that period. It is this consistency that allows me to conclude that Russia's resource allocations and observable behavior were aligned with its stated information security strategy.

Table 5. Comparing and contrasting Russia's words and actions in the information security domain in 2011-2021

Strategic Elements	**Russia's stated InfoSec strategy in 2011-2021**	**Russia's observed actions pertaining to InfoSec in 2011-2021**

End 1	Protect against the threat of the use of ITs to undermine Russia's sovereignty, political and regional stability	Created the National Defense Management Center Command Center and the GosSOPKA system for monitoring and responding to cyberattacks; transformed Roskomnadzor into a powerful surveillance and censorship machine; procured new EW equipment; created EW troops, information operations troops as well as special military units known as "scientific companies;" established new talent pipelines for military information space specialists
End 2	Protect against the threat of Russia's dependence on foreign ITs	Created federal programs, such as "Digital Economy" and "Education Development" to grow the domestic IT sector and develop the IT workforce; introduced legislation limiting the use of foreign ITs by government agencies
End 3	Protect against the threat of subversive information activities aimed at undermining traditional moral, spiritual, and patriotic values	Created cultural and educational programs, such as "Culture Development" to promote patriotic media content and instill said values among the Russian youth
End 4	Protect against the threat of discrimination of the Russian language and media abroad	Sponsored Russian media outlets, such as *RT, Sputnik, TASS, RTR,* and others; expanded the government-controlled media conglomerate internationally; created educational programs for the study of the Russian language abroad
End 5	Protect against the threat of biased assessments of Russian policy	Funded the advancement of Russian media outlets internationally to broadcast in local languages; created its own additional means of information influence abroad via troll factories and other IW means
Means 1	Legal-Administrative	Employed the legal-administrative means of the executive, legislative, judicial, and bureaucratic branches of the government to introduce and enforce policies, laws, and regulations pertaining to InfoSec
Means 2	Military	Employed the means of its military services, such as the GRU, EW troops, information operations troops, as well as special military units known as "scientific companies" to advance InfoSec ends
Means 3	Economic	Utilized its economic means in the form of federal budget allocations, government subsidies, and use of private capital to fund initiatives supporting the stated InfoSec strategy
Means 4	Social-Psychological	Leveraged the social-psychological means of culture and education in the form of federal programs aimed at countering stated information threads
Means 5	Political	Employed the political means of diplomacy in accordance with the stated InfoSec strategy
Way 1	Leverage ITs to strengthen the capabilities of the Russian military and InfoSec services	Created the National Defense Management Center Command Center and the GosSOPKA system for monitoring and responding to cyberattacks; implemented software-hardware site-monitoring system called "Revizor;" procured new EW equipment; created EW troops, information operations troops, as well as special military units known as "scientific companies;" and used Russian military colleges to train new information space specialists
Way 2	Develop domestic IT sectors	Invested in the development of domestic IT sectors; launched federal programs, such as "Digital Economy" aimed at developing a domestic system of IT startups; created vocational training and educational programs for new IT specialists
Way 3	Utilize the spheres of culture and education	Created cultural and educational programs to promote patriotic media content and instill traditional moral, spiritual, and patriotic values among the Russian youth
Way 4	Grow the Russian soft power through the promotion of the Russian media in the global information space	Sponsored Russian media outlets, such as *RT, Sputnik, TASS, RTR,* and others; expanded the government-controlled media conglomerate internationally; created educational programs for the study of the Russian language abroad
Way 5	Control the domestic information environment	Introduced a variety of restrictive laws, regulations, and IT implementations to monitor domestic media and severely restrict the

		freedom of information within the Russian segment of the internet; purged the Russian information space from independent news media, took steps to make the Runet independent from the global internet
Way 6	Shape and define norms of information security and global internet governance via international treaties	Signed numerous InfoSec treaties with members of the CIS, SCO, CSTO, BRICS, and other states; consistently advocated stricter cyberspace regulations across the UN system and beyond; and pushed for a new cybercrime treaty to replace the Budapest Convention

Chapter V.

Conclusion and Future Research

A. Words and Actions of Russia's Information Security Strategy

This study sought to contribute to our understanding of Russia as a strategic geopolitical actor by answering the question: *do Russia's resource allocations and observable behavior in the sphere of information security correspond with its stated strategy in that domain?* To do so, I first used the lens of strategic theory to examine Russia's publicly available doctrinal documents in the 2011-2021 research period to detect key elements of Russia's stated InfoSec strategy, including its *ends, means,* and *ways*.

I established that this strategy aimed at protecting the Russian citizens, society, and the State itself from several specific types of internal and external information threats emanating from Russia's growing confrontation with the West. I also established that, for the purpose of attaining these *ends*, Russia's stated InfoSec strategy prescribed the employment of various legal-administrative, political, economic, social-psychological, and military *means* in six distinct *ways*: (1) leveraging ITs to strengthen the capabilities of the Russian military and InfoSec services; (2) developing domestic IT sectors; (3) utilizing the spheres of culture and education; (4) growing the Russian soft power through the promotion of the Russian media in the global information space; (5) controlling the domestic information environment; and (6) shaping and defining norms of InfoSec and global internet governance via international treaties.

Building on my findings about this triad of *ends, means,* and *ways* of Russia's stated InfoSec strategy, I then formulated thirteen specific propositions regarding the

Russian State's expected behavior in the research period. I proceeded with testing those propositions by comparing them with the government's observable actions in the InfoSec domain, including policies and resource allocations. In the course of this testing, I found that the Russian government generously funded the development of Russia's information communication technology infrastructure, upgrading and enhancing its information warfare capabilities while simultaneously establishing increasingly totalitarian control over its domestic information space by introducing restrictive laws and blocking independent and foreign-funded media.

Overall, I found the Russian State's observable behavior to be surprisingly consistent with its stated InfoSec strategy. In particular, I found that the observed actions of the Russian government in 2011-2021 matched the expected behavior outlined in my propositions. Further, I discovered that Russia's observed actions also aligned with the specific *ends, means*, and *ways* outlined in its stated InfoSec strategy, which I reiterated earlier in the section. In fact, Moscow's actions pertaining to the implementation of this strategy in 2011-2021 can be characterized as methodical, cohesive, and long-term oriented. Perhaps the best illustration of this is Russia's efforts to reshape and redefine established norms of international information security and internet governance. Undeterred by continued opposition from the U.S. and its allies, Russia advocated its vision of cyberspace sovereignty with remarkable consistency. In sum, Russia's sustained long-term commitment to its stated strategy proves that, despite its reputation as an unpredictable and opportunistic actor, Moscow does try to match its words with its actions, at least when it comes to information security.

This thesis both builds on and complements the findings of the scholars that I have highlighted in my literature review. In particular, my research supports the findings of Tashev and McLaughlin (2019) that the Russian leadership exercises a society-wide approach to advancing its InfoSec interests, and that Russia's increasing emphasis on IW is reflected in the government's growing investments in IW capabilities and structures. By examining the activities of the so-called Russian "troll factories," I was able to illustrate how the Russian government employs both national and non-governmental institutions to target not only computer networks but also the views and perceptions of the entire population of the targeted state. Yet, I also discovered that some of Russia's observed IW operations, such as its disinformation campaigns during the 2016 U.S. presidential election, failed to deliver desired results. This complements Moore's (2022) conclusion pertaining to the Russian approach to military offensive network operations, which, according to Moore, often does not yield the desired impact due to technical and operational limitations.

My observations also align with the findings of Grise et al. (2022) that Russia's perception of being in a constant state of information confrontation with the West plays a major role in shaping its foreign policy. Indeed, I found that Russia's foreign policy actions were focused largely on contesting established Western norms pertaining to global internet governance, as well as advancing the Kremlin's vision of a more equitable IIS arrangement. My findings also indicate that the observable actions of the Russian government were largely consistent with the three key elements of Moscow's quest for internet sovereignty identified by Litvinenko (2021). These include: (1) control over data; (2) control over infrastructure; and (3) promotion of the Russian internet governance initiatives at the international level. As explained in Chapter III of this thesis, the Russian government attempted to take control over data by forcing all Russian internet providers to store all internet traffic data within Russian territory. It attempted to take control over infrastructure by developing a national system of the Russian internet that could operate independently from the global internet. Finally, Moscow promoted the Russian internet governance initiatives at the international level by consistently advocating an IIS treaty under the auspices of the UN.

While building on the works of the aforementioned scholars, I have also sought to make my own, if modest, contribution to a holistic understanding of Russia as a unified geopolitical actor in the InfoSec domain. In doing so, I have relied on a variety of original primary evidence that I have collected. This evidence includes official doctrines, decrees, programs, and other documents issued by the Russian government, which I have obtained despite multiple restrictions on foreign users' access to such information that the Russian government has recently introduced. I have also managed to obtain, speeches, and statements by Russian government officials as well as data on Russia's federal budget allocations. The original evidence presented in this thesis also includes official reports by intergovernmental and non-governmental organizations, survey data, government press releases, and texts of international conventions, treaties, and declarations.

While aspiring to expand the existing body of academic knowledge of Russia's behavior in the InfoSec domain, I also hope my thesis's findings may prove to be useful to policymakers in the U.S. and other countries as they seek to expand their understanding of *ends, ways,* and *means* of Russia's increasingly assertive InfoSec strategy in the era of renewed competition among great powers. As the Kremlin has continued to escalate its brinkmanship rhetoric toward the U.S. and the West, it is important that Western policymakers and security specialists understand whether Russia's stated InfoSec strategy can serve as a reliable predictor of its behavior. As these subject-matter experts continue to expand their knowledge of how states put their InfoSec strategies into practice, they will be better equipped to anticipate and defend their countries against future attacks, as well as identify some common rules of the road on IIS. In the meantime, information security remains and will continue to be of increasing importance in all international relations. Therefore, it is important to regularly evaluate how well states match their words with their actions when it comes to their information security strategies and pose fresh questions to explore areas that have not yet been investigated.

B. Future Research

This thesis focused on outlining key elements of Russia's stated information security strategy and testing them against Russia's observable actions in the 2011-2021 period. Even though mine was a single-case study with a relatively short research period, there might be ways one can build on my research to gain further understanding of ways Russia shapes its InfoSec strategy and implements it. For instance, one can explore ways the Russo-Ukrainian War, which Putin unleashed in February 2022, may have impacted the *ends, ways,* and *means* of Russia's InfoSec strategy. One can also explore whether and how this war may have affected the InfoSec strategies of other states, including those that may find themselves in the sphere of Russian information influence. One may ponder, for instance, whether any of these states have implemented any changes in their InfoSec strategies based on Russian tactics and strategies. As part of this post-February

2022 exploration, one could, perhaps, take a closer look at whether the punitive measures, which the West has introduced since February 2022, may have had an impact on Russia's InfoSec strategy. Looking beyond Russia, one can, perhaps, apply the analytical framework, which I have developed and applied for the purposes of this study, to analyze the strategic behavior of other states in the InfoSec domain.

Bibliography

Accounts Chamber of the Russian Federation. “Reiting IT-rashodov federalnyh gosorganov [Rating of the Federal Government IT-spending].” Accessed July 30, 2022. https://spending.gov.ru/analytics/ratings/it/

Aleksey Druzhinin. “Kak menyalos’ nazvanie otechestvennoy razvedki [How the name of the national intelligence changed].” *Press Service of the President/*TASS. November 2, 2018. Accessed October 11, 2022. https://tass.ru/info/5752382

Alexander, Lawrence. “Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign.” *GlobalVoices.org*. April 2, 2015. Accessed July 31, 2022. https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/

Allyn, Bobby. “Study Exposes Russia Disinformation Campaign That Operated In The Shadows For 6 Years.” *NPR*. June 16, 2020. Accessed July 31, 2022. https://www.npr.org/2020/06/16/878169027/study-exposes-russia-disinformation-campaign-that-operated-in-the-shadows-for-6-

Association for Progressive Communications. “Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online.” November 6, 2019. Accessed August 1, 2022. https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human

Atlantic Council of Montenegro. “Russia’s Narratives Toward the Western Balkans: Analysis of Sputnik Srbija.” NATO Strategic Communications Centre of Excellence. April 2020. ISBN: 978-9934-564-24-6. Accessed July 31, 2022. https://stratcomcoe.org/publications/russias-narratives-toward-the-western-balkans-analysis-of-sputnik-srbija/56

Balashova, Anna, Dada Lindell, and Maria Kolomychenko. “Setevoy ‘Revizor’: kak rabotaet sistema kontrolya za zaprewennym kontentom [Network "Inspector": how the control system for prohibited content works].” *RBC.ru.* September 7, 2017. Accessed July 31, 2022. https://www.rbc.ru/technology_and_media/07/09/2017/59b00e269a79475c24ccf0 90

Baranovskaya, Sasha. “Moscow's cyber-defense: How the Russian government plans to protect the country from the coming cyberwar.” *Meduza*. July 19, 2017. Accessed July 30, 2022. https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense

Barnes, Julian E. “Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say.” *The New York Times*. Published July 16, 2020, updated December 14, 2020. Accessed February 5, 2023. https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html

BBC. “Chislo SMI-‘inoagentov’ v Rossii prevysilo 100 [The number of media-‘foreign agents’ in Russia exceeded 100].” December 3, 2021. Accessed February 6, 2023. https://www.bbc.com/russian/news-59011912

———“Gosduma prinyala zakon o priznanii zarubezhnyh CMI inoagentami [The State Duma adopted a law on the recognition of foreign media as foreign agents].” November 15, 2017. Accessed July 31, 2022. https://www.bbc.com/russian/news-41994050

———“Putin obvinyaet SSHA v provocirovanii protestov [Putin accuses USA in provoking protests].” December 8, 2011. Accessed July 28, 2022. https://www.bbc.com/russian/russia/2011/12/111208_putin_opposition_protests

———“Putin ogranichil innostrannye doli v rossiyskih SMI [Putin limited foreign stakes in Russian media].” October 15, 2014. Accessed July 31, 2022. https://www.bbc.com/russian/russia/2014/10/141015_putin_media_foreign

———“Putin podpisal zakon o ‘suverennom internete.’ On vstupit v silu cherez polgoda [Putin signed the law on the ‘sovereign Internet.’ It will come into effect in six months.].” May 1, 2019. Accessed July 31, 2022. https://www.bbc.com/russian/news-48126218

Belarusian Telegraph Agency (BelTA). “Belarus, Russia to expand cooperation in information security.” September 10, 2019. Accessed January 15, 2023. https://eng.belta.by/politics/view/belarus-russia-to-expand-cooperation-in-information-security-124031-2019/

Belyaeva, Yana. “‘Skolkovo’: chto vyshlo iz proekta rossiyskoy Kremnievoy doliny [‘Skolkovo’: what came of the Russian Silicone Valley project].” *Deutsche Welle (DW).* October 27, 2019. Accessed July 30, 2022. https://bit.ly/3DYrH68

Bernal, Alonso, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla. “Cognitive Warfare: An Attack on Truth and Thought.” NATO and Johns Hopkins University. 2020.

Berzinš, Janis. “Russia’s New Generation Warfare In Ukraine: Implications For Latvian Defense Policy.” National Defence Academy of Latvia. Center for Security and Strategic Research. Policy Paper #02. April 2014.

Boletskaya, Kseniya and Mari Mesropya. “Operatory otkluchayut ‘Dojd’ po vsey strane [Operators turn off "Rain" throughout the country].” *Vedomosti.* January 29, 2014. Accessed July 31, 2022. https://www.vedomosti.ru/technology/articles/2014/01/29/operatory-otklyuchayut-dozhd-po-vsej-strane

Borodina, Arina. “Televidenie stanet raznodostupnym [Television will become widely available].” *Kommersant.* August 23, 2012. Accessed July 31, 2022. https://www.kommersant.ru/doc/2006556

Borzenko, Aleksandr. "'Paket Yarovoy' prinyat bolshe polugoda nazad. Kak on rabotaet? ['The Yarovaya Package' was adopted more than six months ago. How does he work?]." *Meduza.io.* February 13, 2017. Accessed July 31, 2022. https://meduza.io/feature/2017/02/13/zakon-yarovoy-prinyat-bolshe-polugoda-nazad-kak-on-rabotaet

Bowen, Andrew S. "Russian Cyber Units." Congressional Research Service. IF11718, Version 4. Updated February 2, 2022. Accessed July 30, 2022. https://crsreports.congress.gov/product/details?prodcode=IF11718

Bowen, Glenn, A. "Document Analysis as a Qualitative Research Method." *Qualitative Research Journal,* vol. 9, no. 2, 2009. ISSN: 1443-9883. Accessed August 17, 2022. https://www.emerald.com/insight/content/doi/10.3316/QRJ0902027/full/html

BRICS Leaders Meeting. *Brasilia Declaration.* Brasilía, Brazil, November 14, 2019. Accessed January 1, 2023. http://www.brics.utoronto.ca/docs/191114-brasilia.html

———*Fortaleza Declaration*. Fortaleza, Brazil, July 15, 2014. Accessed January 1, 2023. http://www.brics.utoronto.ca/docs/140715-leaders.html

———*Moscow Declaration*. Moscow, the Russian Federation, November 17, 2020. Accessed February 27, 2023. http://www.brics.utoronto.ca/docs/201117-moscow-declaration.html

———*New Delhi Declaration*. New Delhi, India, September 9, 2021. Accessed February 27, 2023. http://www.brics.utoronto.ca/docs/210909-New-Delhi-Declaration.html

———*Sanya Declaration*. Sanya, Hainan, China, April 14, 2011. Accessed January 1, 2023. http://in.china-embassy.gov.cn/eng/xwfw/xxfb/201104/t20110415_2373458.htm

———*Ufa Declaration*. Ufa, the Russian Federation, July 9, 2015. Accessed January 1, 2023. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/201507/t20150717_679402.html

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford University Press; 1st edition (February 1, 2017). ISBN-10: 0190665017.

———*The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Harvard University Press; 1st edition. February 25, 2020. ISBN-10: 0674987551.

Bugayova, Nataliya, Mason Clark, Michaela Walker, Andre Briere, Anthony Yanchuk, and George Barros. "The Kremlin's Inroads after the Africa Summit." Institute for the Study of War. November 8, 2019. Accessed January 15, 2023.

http://www.understandingwar.org/backgrounder/kremlins-inroads-after-africa-summit

C-News. "Byvshuu IB-kompaniu FSB prevratili v akcionernoe obwestvo [Former FSB cybersecurity company was turned into a joint-stock company]." September 22, 2020. Accessed July 30, 2022. https://www.cnews.ru/news/top/2020-09-22_byvshuyu_ibkompaniyu_fsbotdannuyu

———"Iz gosprogrammy 'Informacionnoe obwestvo' udalyaut punkt o tehnologicheskoy nezavisimosti Rossii [The item on the technological independence of Russia is removed from the state program 'Information Society']." December 28, 2016. Accessed July 31, 2022. https://www.cnews.ru/news/top/2016-12-28_minkomsvyazi_otkazalos_ot_dostizheniya_tehnezavisimosti

———"'Rostelekom' podvel itogi ekspluatacii Severnogo opticheskogo potoka [Rostelecom summed up the operation of the Nord Optical Stream]." April 14, 2016. Accessed July 31, 2022. https://www.cnews.ru/news/line/2016-04-14_rostelekom_podvel_itogi_ekspluatatsii_severnogo

———"V Rossii nachalis massovye uvolneniya rukovoditelei gosudarstvennoi cifrovoi transformacii [Mass layoffs of heads of the state digital transformation began in Russia]." January 27, 2021. Accessed July 30, 2022. https://www.cnews.ru/news/top/2021-01-27_v_rossii_nachalis_massovye

———"Vybrany centry proryvnyh IT-issledovaniy, kotorye poluchat gospodderzhku [Centers for breakthrough IT research have been selected to receive state support]." November 27, 2013. Accessed July 31, 2022. https://www.cnews.ru/news/top/vybrany_tsentry_proryvnyh_itissledovanij

Cambridge University Press, s.v. "soft power." Cambridge Advanced Learner's Dictionary & Thesaurus. Cambridge University Press, n.d. Accessed February 4, 2023. https://dictionary.cambridge.org/dictionary/english/soft-power

Chebakova, Darya and Anna Balashova. "V Rossii protestirovali rabotu Runeta pri otkluchenii ot globalnoy Seti. Okonchatelnye itogi budut podvedeny cherez mesyac, seychas dannyh o sboyah net [In Russia, the operation of the Runet when disconnected from the global network was tested. Final results will be summed up in a month, currently there are no data on failures]." *RBC.ru*. July 21, 2021. Accessed July 31, 2022. https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739

Chekinov, Sergei G. and Sergei A. Bogdanov. "Priroda I soderzhanie voiny novogo pokoleniya [The nature and content of the new generation of war]." *Voennaya Mysl'* [*The Military Thought*]. 4 (2013): 12-23.

Chernenko, Elena. "Belorussiya vybrala internet pobezopasnee [Belarus chose a safer internet]." *Kommersant.* June 7, 2012. Accessed July 31, 2022. https://www.kommersant.ru/doc/1953059

Chernenko, Elena. "V MIDe poyavilsya curator interneta [The Ministry of Foreign Affairs got an internet curator]." *Kommersant.* March 20, 2012. Accessed August 1, 2022. https://www.kommersant.ru/doc/1896438

Chesnokov, Evgeny. "Skolkovo Stroitsya [Skolkovo is being built]." *Russkiy Bloger* (blog) [*Russian Blogger*]. July 3, 2018. Accessed July 30, 2022. https://rblogger.ru/2018/07/03/skolkovo/

Council of Europe. Details of Treaty No.185. Accessed July 31, 2022. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

———Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. Accessed July 30, 2022. https://www.coe.int/en/web/cybercrime/parties-observers

Creswell, John W., and Cheryl N. Poth. *Qualitative Inquiry & Research Design: Choosing Among Five Approaches*. Fourth edition. Los Angeles: SAGE, 2018.

Crowdstrike. "CrowdStrike's work with the Democratic National Committee: Setting the record straight." June 5, 2020. Accessed July 30, 2022. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Cunningham, Conor. "A Russian Federation Information Warfare Primer." The Henry M. Jackson School of International Studies. University of Washington. November 12, 2020. Accessed July 30, 2022. https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/#_ftn11

Curtis, Glenn and Jim Nichol. *Annotated Bibliography on Psychological Operations*, Federal Research Division Library of Congress, April 1989. Accessed February 2022. https://apps.dtic.mil/sti/pdfs/ADA302447.pdf

Department of Information and Communications Technology, Republic of the Philippines. "DICT, Russian company to cooperate on cybersecurity initiatives." September 25, 2018. Accessed January 11, 2023. https://dict.gov.ph/dict-russian-company-to-cooperate-on-cybersecurity-initiatives/

Eady, Gregory, Tom Paskhalis, Jan Zilinsky, Richard Bonneau, Jonathan Nagler, and Joshua A. Tucker. "Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior." *Nature Communications* 14, 62 (2023). Accessed February 6, 2023. https://doi.org/10.1038/s41467-022-35576-9

Erlanger, Steven. “Russia’s RT Network: Is It More BBC or K.G.B.?” *The New York Times.* March 8, 2017. Accessed July 31, 2022. https://www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html

European Union Agency for Cybersecurity. National Cybersecurity Strategies. Accessed July 28, 2022. https://www.enisa.europa.eu/topics/national-cyber-security-strategies

Federal Service for Supervision of Communications, Information Technology and Mass Media (abbr. Roskomnadzor), Russian Federation. “Ogranichen dustup k ryadu internet-resursov, rasprostranyavshih prizyvy k nesankcionirovannym massovym meropriyatiyam [Access to a number of Internet resources that disseminated calls for unauthorized mass events was restricted].” March 13, 2014. Accessed July 31, 2022. http://rkn.gov.ru/news/rsoc/news24447.htm

Federation Council of the Federal Assembly of the Russian Federation. *Cyber Security Strategy Concept of the Russian Federation*. November 29, 2013. Accessed October 20, 2022. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

Finkle, Jim. “Researchers say Stuxnet was deployed against Iran in 2007.” Reuters. February 26, 2013. Accessed January 28, 2023. https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226

Freedom on the Net 2021: Russia. FreedomHouse.org. Accessed July 31, 2022. https://freedomhouse.org/country/russia/freedom-net/2021

Gady, Franz-Stefan and Greg Austin. “Russia, The United States, And Cyber Diplomacy: Opening the Doors.” EastWest Institute. 2010. Accessed July 31, 2022. https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf

Galeotti, Mark. “I’m Sorry for Creating the ‘Gerasimov Doctrine.’” *Foreign Policy*. March 5, 2018. Accessed January 2, 2023. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

———“Putin’s Hydra: Inside Russia’s Intelligence Services.” European Council on Foreign Relations. Policy Brief. May 2016. Accessed July 30, 2022. https://bit.ly/41ak9Y4

———“Rossiyskaya Razvedka Vedet (Politicheskyu) Voinu [Rusian Intelligence Conducts (Political) War].” *The NATO Review*. May 12, 2017. Accessed July 30, 2022. https://www.nato.int/docu/review/ru/articles/2017/05/12/rossijskaya-razvedka-vedet-politicheskuyu-vojnu/index.html

Garmazhapova, Aleksandra. “Gde zhivut trolli. I kto ih kormit [Where trolls live. And who feeds them].” *Novaya Gazeta* [*New Gazette*]. September 7, 2013. Accessed

July 31, 2022. https://novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit

Gazeta.ru. “Naznachen novyi zamministra oborony [New deputy defense minister appointed].” November 24, 2008. Accessed July 28, 2022. https://www.gazeta.ru/news/lenta/2008/11/24/n_1300007.shtml

Gerasimov, Valery. “Cennost’ nauki v predvidenii [The Value of Science is in the Foresight].” *Voenno-Promyshlennyi Kur’er* [*The Military-Industrial Courier*]. February 26, 2013. Accessed July 30, 2022. https://vpk-news.ru/articles/14632

———“The Value of Science Is in the Foresight.” *Military Review*. 2016: January–February. pp. 23-29. Accessed July 30, 2022. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/

Giles, Keir and Akimenko, Valeriy. “Russia’s Cyber and Information Warfare.” *Asia Policy*. 2020. Roundtable: The Future of Cybersecurity across the Asia-Pacific. Accessed July 30, 2022. https://www.academia.edu/42893415/Russia_s_Cyber_and_Information_Warfare?auto=citations&from=cover_page

Giles, Keir. “Handbook Of Russian Information Warfare.” NATO Defense College. November 2016. ISBN: 9788896898161. Accessed July 28, 2022. https://www.researchgate.net/publication/313423985_Handbook_of_Russian_Information_Warfare

———“‘Information Troops’ – a Russian Cyber Command?” 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011 © CCD COE Publications.

———“Russia’s ‘New’ Tools for Confronting the West: Continuity and Innovation in Moscow’s Exercise of Power.” Chatham House. The Royal Institute of International Affairs. March 2016. Accessed July 28, 2022. https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power

———“Russia’s Public Stance on Cyberspace Issues.” 2012 4th International Conference on Cyber Conflict. C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 © NATO CCD COE Publications, Tallinn.

Government of the Russian Federation. Postanovlenie Pravitelstva RF ot 15 aprelya 2014 g. N 295 “Ob utverzhdenii gosudarstvennoy programmy Rossiyskoy Federacii ‘Razvitie obrazovaniya’ na 2013-2020 gody [Decree of the Government of the Russian Federation of April 15, 2014, N 295 “On Approval of the State Program of the Russian Federation ‘Education Development’ for 2013-2020”].” p.9. Accessed July 31, 2022. https://base.garant.ru/70643472/

———Postanovlenie Pravitelstva RF ot 15 aprelya 2014 g. N 317 “Ob Utverzhdenii gosudarstvennoy programmy Rossiyskoy Federacii ‘Razvitie kultury’ [Decree of the Government of the Russian Federation of April 15, 2014, N 317 “On approval of the state program of the Russian Federation ‘Development of culture’”].” Accessed July 31, 2022. http://gov.garant.ru/SESSION/PILOT/main.htm

———Postanovlenie Pravitelstva RF ot 20 avgusta 2013 g. N 718 “O federalnoy celevoy programme ‘Ukrepleniye edinstva rossiyskoy nacii i etnokulturnoe razvitie narodov Rossii (2014-2020 gody)’ [Decree of the Government of the Russian Federation of August 20, 2013, N 718 “On the federal target program ‘Strengthening the unity of the Russian nation and the ethno-cultural development of the peoples of Russia (2014 - 2020)’”].” Accessed July 31, 2022. https://base.garant.ru/70439260/

———Postanovlenie Pravitelstva RF ot 5 May 2016 g. N 392 “O prioritetnyh napravleniyah ispolzovaniya i razvitiya informacionno-kommunikacionnyh tehnologiy v federalnyh organah ispolnitelnoi vlasti i organah upravleniya gosudarstvennymivnebudjetnymi fondami i o vnesenii izmeneniy v nekotorye akty Pravitelstva Rossiyskoy Federacii [Decree of the Government of the Russian Federation of May 5, 2016 N 392 “On priority areas for the use and development of information and communication technologies in federal executive bodies and management bodies of state extra-budgetary funds and on amendments to some acts of the Government of the Russian Federation”].” Accessed July 30, 2022. https://base.garant.ru/71394834/#block_12

———Postanovlenie Pravitelstva Rossiyskoy Federacii ot 01.11.2021 g. No.1897 [Government of the Russian Federation resolution of November 1, 2021, No.1897]. Accessed July 31, 2022. http://government.ru/docs/all/137420/

———Rasporyazhenie ot 13 avgusta, 2013 g. N 1414-r “O dopolnenii gosudarstvennoi programmy ‘Ekonomicheskoe razvitie i inovacionnaya ekonomika’ [Order from August 13, 2013, No 1414-r “On expansion of the state program ‘Economic development and innovative economy’”].” Accessed July 30, 2022. http://government.ru/docs/3843/

———Rasporyazhenie ot 22 Noyabrya 2012 g. No 2148-r: “Ob utverzhdenii gosudarstvennoy programmy Rossiyskoy Federacii ‘Razvitie obrazovaniya’ na 2013-2020 gody [Decree of November 22, 2012, No 2148-r: “On approval of the government program of the Russian Federation ‘Education Development’ for 2013-2020”].” Accessed January 11, 2023. http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf 9

———Rasporyazhenie ot 28 iulya 2017 g. No 1632-r: “Utverdidt prilagaemuu programmu ‘Cifrovaya Ekonomika Rossiyskoy Federacii’ [Order from July 28, 2017, No 1632-r: “Approve the attached program ‘Digital Economy of the Russian Federation’”].” Accessed July 30, 2022.

http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

———Rasporyazhenie Pravitelstva RF ot 2 dekabrya 2011 g. No 2161-r: "Gosudarstvennaya programma Rossiyskoy Federacii 'Informacionnoe Obwestvo' (2011-2020 gody) [Decree of the Government of the Russian Federation of December 2, 2011, N 2161-r: "Government Program of the Russian Federation 'Information Society' (2011 - 2020)"]." Accessed July 31, 2022. http://www.pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102142714&backlink=1&&nd=102152835

———"Sovmestnoe zayavlenie prezidentov Rossiyskoy Federacii I Soedinennyh Shtatov Ameriki o novoy oblasti sotrudnichestva v ukreplenii doveriya [Joint Statement by the Presidents of the Russian Federation and the United States of America on a New Area of Confidence-Building Cooperation]." June 17, 2013. Accessed January 2, 2023. http://kremlin.ru/supplement/1479

———*The Maritime Doctrine of the Russian Federation.* 2015. Accessed August 30, 2022. https://digital-commons.usnwc.edu/rmsi_research/3

———*The Military Doctrine of the Russian Federation*. February 5, 2010. Accessed January 2, 2023. https://carnegieendowment.org/files/2010russia_military_doctrine.pdf

———*The Military Doctrine of the Russian Federation.* No.Pr.-2976, December 25, 2014.

———Ukaz Presidenta RF ot 10 oktyabrya 2019 g. N 490 "O razvitii iskustvennogo intellekta v Rossiyskoy Federacii [Presidential Decree of October 10, 2019, N 490 "On the development of artificial intelligence in the Russian Federation"]." Government of the Russian Federation. Accessed July 30, 2022. https://base.garant.ru/72838946/

———"Vstrecha Mihaila Mishustina s zamestitelyami rukovoditelei federalnyh organov ispolnitelnoi vlasti, otvetstvennymi za cifrovuu transformaciu [Mikhail Mishustin's meeting with deputy heads of federal executive bodies responsible for digital transformation]." March 12, 2020. Accessed July 30, 2022. http://government.ru/news/39129/

Gray, Colin S. *Theory of Strategy*. Oxford University Press. 2018. ISBN-10: 0198800673.

Grise, Michelle, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska. "Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation," RAND Corporation. 2022. ISBN: 978-1-9774-0717-7. Accessed August 29, 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA198-8/RAND_RRA198-8.pdf

Habibrahimov, Albert. “Putin podpisal zakon ob uzhestochenii kontrolya za SIM-kartami [Putin signed a law on tightening control over SIM-cards].” *VC.ru*. July 31, 2017. Accessed July 31, 2022. https://vc.ru/flood/25550-putin-sim

Hachatryan, Diana. “Kak stat’ trollhanterom [How to become a troll hunter].” *Novaya Gazeta* [*New Gazette*]. March 10, 2015. https://novayagazeta.ru/articles/2015/03/10/63342-kak-stat-trollhanterom (accessed July 31, 2022); also, see: Chen, Adrian. “Agenstvo [The Agency].” *The New York Times*. June 4, 2015. Accessed July 31, 2022. https://www.nytimes.com/2015/06/07/magazine/the-agency-russian.html#commentsContainer

Haugen, H. M. “The crucial and contested global public good: principles and goals in global internet governance.” *Internet Policy Review*, 9(1). 2020. Accessed July 30, 2022. https://doi.org/10.14763/2020.1.1447

Heffington, Steven, Adam Oler, and David Tretler. *A National Security Strategy Primer.* National Defense University Press, Washington, D.C. 2019. Accessed December 18, 2022. https://bit.ly/3Ia1nr7

Hogeveen, Bart, “The UN norms of responsible state behaviour in cyberspace.” Australian Strategic Policy Institute (ASPI), International Cyber Policy Centre. March 22, 2022. Accessed August 1, 2022. https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

Igor Lyapunov, Biography. Roskongress. Accessed January 11, 2023. https://roscongress.org/speakers/lyapunov-igor/biography/

“Integral,” a research and production complex. “Analiz federalnogo budzheta na razvitie informacionnyh tehnologiy: nastoyawee I buduwee [Analysis of the federal budget for the development of information technologies: the present and the future].” September 26, 2017. Accessed July 30, 2022. https://integral-russia.ru/2017/09/26/analiz-federalnogo-byudzheta-2017-goda-na-razvitie-informatsionnyh-tehnologij/

Interfax. “Genshtab vozglavil Valeriy Gerasimov [Valery Gerasimov takes the helm of the General Staff].” November 9, 2012. Accessed July 30, 2022. https://www.interfax.ru/russia/275082

———“V Gosdume oprovergli suwestvovanie “kibervoysk” v Rossii [The State Duma denied the existence of "cyber troops" in Russia].” January 16, 2017. Accessed February 12, 2023. https://www.interfax.ru/russia/545640

———“V Minoborony RF sozdali voiska informacionnyh operacyi [The Russian Ministry of Defense created the information operations troops].” February 22, 2017. Accessed via the Wayback Machine July 30, 2022. https://web.archive.org/web/20220516105752/https://www.interfax.ru/russia/551054

Interior Ministry of the Russian Federation. “Upravlenie ‘K’ MVD Rossii [Directorate ‘K’ MVD Russia].” Archived June 14, 2015. Accessed via the Wayback Machine February 14, 2023. https://bit.ly/3Z7rQMR

Internet Corporation for Assigned Names and Numbers (ICANN). “Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends.” October 1, 2016. Accessed July 30, 2022. https://go.icann.org/3Icty8D

*ISPreview. “*2022 vs 2021 – UK Broadband and Mobile Speeds vs the World.” December 29, 2022. Accessed March 7, 2023. https://www.ispreview.co.uk/index.php/2022/12/2022-vs-2021-uk-broadband-and-mobile-speeds-vs-the-world.html

Istomina, Maria. “Reklama v internete vpervye obognala TV [Online advertising overtakes TV for the first time].” *RBC.ru.* March 11, 2019. Accessed July 31, 2022. https://www.rbc.ru/technology_and_media/11/03/2019/5c8619ce9a79473741c1055f

Jervis, Robert. “Cooperation Under the Security Dilemma.” *World Politics* 30, no. 2 (1978): 167–214. Accessed October 15, 2022. https://doi.org/10.2307/2009958

Jibilian, Isabella and Canales, Katie. “The US is readying sanctions against Russia over the SolarWinds cyberattack. Here's a simple explanation of how the massive hack happened and why it's such a big deal.” *Business Insider*. April 15, 2021. Accessed January 29, 2022. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Jones, Frank, L. “Toward a Strategic Theory of Terrorism: Defining Boundaries in the Ongoing Search for Security.” *Strategic Studies Institute, US Army War College.* 2012. Accessed August 17, 2022. https://www.jstor.org/stable/pdf/resrep12116.11.pdf

Kahler, Miles. “Rationality in International Relations.” *International Organization* 52, no. 4 (1998): 919–41. Accessed March 7, 2023. http://www.jstor.org/stable/2601362

Kapur, Arjun and Simon Saradzhyan. “For Russia and America, Election Interference Is Nothing New: 25 Stories.” Belfer Center for Science and International Affairs, Harvard Kennedy School. March 22, 2017. Accessed March 7, 2023. https://www.russiamatters.org/analysis/russia-and-america-election-interference-nothing-new-25-stories

Kasyanova, Nadezhda. “Deputaty predlozhili ogranichit’ innostrannoe uchastie v rossiyskih CMI [Deputies proposed to limit foreign participation in Russian media].” *E1.ru.* September 17, 2014. Accessed July 31, 2022. https://www.e1.ru/text/gorod/2014/09/17/52892691/

Kirillova, Elina. “Zapuskaetsya programma po sozdaniyu issledovatelskih centrov v oblasti IT [A program is being launched to create research centers in the field of IT].” *RB.ru*. July 31, 2013. Accessed July 31, 2022. https://rb.ru/news/Zapuskaetsya-programma-po-sozdaniyu-issledovatelskih-centrov-v-oblasti-it/

Kiselev, V. and A. Kostenko. “Kibervoyna kak osnova gibridnoy operatsii [Cyberwar as the Basis of Hybrid Operations].” *Armeiskii Sbornik* 257, no. 11 (November 2015):3–6. Accessed January 11, 2023. http://www.oboznik.ru/?p=45314

Kjellen, Jonas. “Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces.” The Ministry of Defense of Sweden. Report no FOI-R-4625-SE. September 2018.

Kolomychenko, Maria. “V internet vveli kibervoiska [Cybertroops have entered the internet].” *Kommersant*. January 10, 2017. Accessed July 30, 2022. https://www.kommersant.ru/doc/3187320

Korchenkova, Natalya. “U ‘Eha Moskvy’ poyavilsya novyi generalnyi director [Ekho Moskvy has a new CEO].” *Kommersant.* February 18, 2014. Accessed July 31, 2022. https://www.kommersant.ru/doc/2410985

Korotkov, Denis. “Sotni trollei za million [Hundreds of trolls for millions].” *Fontanka.ru.* May 29, 2014. Accessed July 31, 2022. https://www.fontanka.ru/2014/05/29/170/

Korzak, Elaine. “Russia’s Cyber Policy Efforts in the United Nations.” NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Tallinn Paper No.11 2021. Accessed July 31, 2022. https://www.ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf

Kotlyar, Evgeniya. “‘U nas byla cel’…vyzvat’ besporyadki’: intervju s eks-sotrudnikom ‘fabriki trolley’ v Sankt-Peterburge [‘We had a goal ... to cause unrest’: an interview with an ex-employee of the ‘troll factory’ in St. Petersburg].” *Telekanal Dojd’* [*TV Rain*]. October 14, 2017. Accessed July 31, 2022. https://tvrain.ru/teleshow/bremja_novostej/fabrika-447628/

Kotlyarov, Maksim V. “Kontroliruya Nekontroliruemoe: Strategiya Rossiyskogo Gosudarstva v Internete [Controlling the Uncontrollable: the Russian Government’s Internet Strategy].” *Vestnik Permskogo Universiteta* [*Perm University Courier*]. *Politology*. 2017. №3. Accessed August 14, 2022. https://cyberleninka.ru/article/n/kontroliruya-nekontroliruemoe-strategiya-rossiyskogo-gosudarstva-v-internete

Kucharski, Lesley. “Russian Multi-Domain Strategy against NATO: information confrontation and U.S. forward-deployed nuclear weapons in Europe.” Lawrence Livermore National Lab. (LLNL), Livermore, CA (United States). 2019. Accessed December 24, 2022. https://www.osti.gov/biblio/1635758

Kurowska, Xymena. “What does Russia want in cyber diplomacy? A primer.” Central European University. EU Cyber Direct Research Paper. December 2019. Accessed July 31, 2022. https://www.ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf

Kuvshinova, Olga. “Pravitelstvo v tretiy raz zamorozilo nakopitelnye pensionnye vznosy [The government froze funded pension contributions for the third time].” *Vedomosti.* September 29, 2015. Accessed July 31, 2022. https://www.vedomosti.ru/economics/articles/2015/09/29/610770-pravitelstvo-medvedeva-zamorozilo

Lapik, Igor. “Serdce rossiyskoi armii: kak rabotaet nacionalny centr upravleniya oboronoi [The Heart of the Russian Army: How the National Defence Center operates].” *Zvezda TV* [*Star TV*]. December 19, 2019. Accessed July 30, 2022. https://tvzvezda.ru/news/201912191737-JcWFf.html

Latsinskaya, Maria, Aleksandr Braterskiy, and Ignat Kalinin. “Rossiya vvela voiska v internet [Russia Sent Troops onto the Internet].” *Gazeta.ru*. 22 February 2017. Accessed July 30, 2022. https://www.gazeta.ru/tech/2017/02/22_a_10539719.shtml

Lebedev, P.A., Kazaryan K.R., Chistov D.M., Petuhova S.I., Gorshkov T., Makarova A.R., Radkevich A.L., Alieva V., Yakovenchuk D.V., Yuryev M., Morozova A.V., Golikova L.B., Novozhilova M.A., Ovchinnikov B.V. “Internet v Rossii: Sostoyanie, tendencii i perspektivy razvitiya [Internet in Russia: current state, tendencies and development prospects].” Federalnoye agenstvo po pechati i massovym kommunikacyam. Upravlenie teleradiovewaniya i sredstv massovyh kommunikacyi [Federal Agency of Press and Mass Communications. Directorate of Broadcasting and Mass Communications]. 2011. ISBN 978-5-904427-15-3. Accessed July 31, 2022. https://raec.ru/activity/analytics/10122/

Lenta.ru. “Anatomiya sliva protesta. Kremlevskie eksperty vyyasnili, pochemu na mitingi hodit vse menshe ludei [Anatomy of a protest drain. Kremlin experts have found out why fewer people go to rallies].” December 6, 2012. Accessed July 31, 2022. https://lenta.ru/articles/2012/12/06/protest1/

———“Pervye nauchnye roty otpravilis’ na sluzhbu [The first scientific companies went to serve].” July 9, 2013. Accessed February 5, 2023. https://lenta.ru/news/2013/07/09/companies/

Lewis, James A. “Cognitive Effect and State Conflict in Cyberspace*.” Center for Strategic and International Studies (CSIS).* September 26, 2018. Accessed December 11, 2022. https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace

Likhonosov, Aleksandr G. “Schastie – luybit svou rodinu. Patrioticheskoe vospitanie grazhdan strany kak osnova informacionnoy bezopasnosti gosudarstva [Happines is to love your homeland! Patriotic education of citizens of the country as the basis of information security of the state].” *Vestnik Voennogo Obrazovaniya* [*Military Education Courier*]. May-June 2021 No.3 (30). Accessed July 31, 2022. https://bit.ly/3lCG6yv

Lilly, Bilyana and Joe Cheravitch. “The Past, Present, and Future of Russia’s Cyber Strategy and Forces.” 2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.). 2020 © NATO CCDCOE Publications, Tallinn.

Lindell, Dada and Nikolai Yaroshenko. “SMI ne nuzhny. Za vosem let chislo vydavaemyh RKN licenziy sokratilos bolee chem v dva raza. Issledovanie ‘MBH Media’ [The media are not needed. Over eight years, the number of licenses issued by the RKN has more than halved. MBH media research.].” *MBK News*. July 9, 2021. Accessed July 31, 2022. https://mbk-news.appspot.com/sences/smi-ne-nuzhny/

Litvinenko, Anna. “Re-Defining Borders Online: Russia’s Strategic Narrative on Internet Sovereignty.” *Media and Communication.* (ISSN: 2183–2439) 2021, Volume 9, Issue 4, Pages 5–15. Accessed August 14, 2022. https://doi.org/10.17645/mac.v9i4.4292

Lomakina, Yana. “Kogo I za chto rossiyskiye vlasti vkluchili v reestr SMI-inostrannyh agentov – spisok Minjusta (obnovlyaemyi) [Whom and why did the Russian authorities include in the register of media-foreign agents - the list of the Ministry of Justice (updated)].” *TJournal.ru.* July 16, 2021. Accessed February 6, 2023. https://tjournal.ru/analysis/410978-kogo-i-za-chto-rossiyskie-vlasti-vklyuchili-v-reestr-smi-inostrannyh-agentov-spisok-minyusta-obnovlyaemyy

Luzin, Pavel. “Rossiyskie kibervoiska: celi i protivorechiya [Russian cyber troops: goals and contraditions].” *Riddle.io*. April 28, 2021. Accessed July 30, 2022. https://ridl.io/rossijskie-kibervojska-celi-i-protivorechija/

Maida, Adam. “Onlain I po vsem frontam. Nastuplenie na svobodu vyrazheniya mneniy v Rossii [Online and on all fronts. Attack on freedom of expression in Russia].” Human Rights Watch. July 18, 2017. Accessed July 31, 2022. https://www.hrw.org/ru/report/2017/07/18/306656

Markoff, John and Andrew E. Kramer. “U.S. and Russia Differ on a Treaty for Cyberspace.” *The New York Times*. June 27, 2009. Accessed July 30, 2022. https://www.nytimes.com/2009/06/28/world/28cyber.html

Merriam-Webster, s.v. “Ransomware.” *Merriam-Webster.com dictionary*. Accessed February 5, 2022. https://www.merriam-webster.com/dictionary/ransomware

Mescheryakov, Vladislav. “Pred’yavlyat pasport dlya dostupa k Wi-Fi v parkah i kafe ne potrebuetsya [You won’t need to show your passport to access Wi-Fi in parks and cafes].” *C-News.* August 8, 2014. Accessed July 31, 2022. https://safe.cnews.ru/news/top/predyavlyat_pasport_dlya_dostupa_k_wifi

Metcel, Mikhail. “Putin podpisal ukaz o sozdanii voennogo tehnopolisa ‘Era’ v Anape [Putin signed a decree on the creation of military technopolis ‘Era’ in Anapa].” TASS. June 25, 2018. Accessed July 30, 2022. https://tass.ru/armiya-i-opk/5322634

Ministry of Defense of the Russian Federation. *Dictionary of Terms*, s.v. “Informatsionnoe protivoborstvo [Information confrontation].” Accessed February 5, 2022. http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary

———*Dictionary of Terms*, s.v. “Informatsionnye tehnologii [Information technologies],” Accessed October 22, 2022. https://dictionary.mil.ru/folder/123100/letter/9/

———*Dictionary of Terms*, s.v. “Radioelektronnaya borba (REB) [Radio electronic struggle],” Accessed October 22, 2022. https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14416@morfDictionary

———*Russian Federation Armed Forces’ Information Space Activities Concept*. 2011. Accessed February 5, 2022. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

———*Strategy of National Security of the Russian Federation*. July 2, 2021. Accessed November 7, 2022. https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf

Ministry of Digital Development, Telecommunications and Mass Media of the Russian Federation. “Gosudarstvennye infosistemy budut finansirovatsya po otdelnomu kodu rashodov [Government info-systems will be financed according to a separate cost code].” July 28, 2020. Accessed July 30, 2022. https://digital.gov.ru/ru/events/39978/

———“Rossiyskaya kompaniya pomozhet V’etnamu v sozdanii antivirusa dlya gosorganov [Russian company will help Vietnam create antivirus for government agencies].” August 7, 2019. Accessed January 11, 2023. https://digital.gov.ru/ru/events/39250/

Ministry of Foreign Affairs of the Russian Federation. *Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence.* June 2, 2020. Accessed February 27, 2023. https://archive.mid.ru/en/web/guest/foreign_policy/international_safety/disarmament/-/asset_publisher/rp0fiUBmANaH/content/id/4152094

———*Doctrine of Information Security of the Russian Federation*. December 5, 2016. Accessed October 22, 2022. https://publicintelligence.net/ru-information-security-2016/

———*Foreign Policy Concept of the Russian Federation.* December 2016. Accessed February 27, 2023. https://www.voltairenet.org/article202038.html

———*Konseptsiya vneshnei politiki Rossiiskoi Federatsii* [*Foreign Policy Concept of the Russian Federation*]. February 12, 2013. Accessed October 30, 2022. https://www.rusemb.org.uk/in1/

———*Konseptsiya vneshnei politiki Rossiiskoi Federatsii* [*Foreign Policy Concept of the Russian Federation*]. November 30, 2016. Accessed October 30, 2022. https://www.rusemb.org.uk/rp_insight/

———"Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security." September 4, 2017. Accessed January 15, 2023. https://archive.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2854430

———*Russian Draft Convention on International Information Security*. September 22, 2011. Accessed July 31, 2022. https://bit.ly/3ZCGhJd

———"Soglashenie mezhdu Pravitel'stvom Rossiyskoy Federacii i Pravitel'stvom Respubliki Kuba o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informacionnoy bezopasnosti [Agreement between the Government of the Russian Federation and the Government of the Republic of Cuba on cooperation in providing international information security]." July 11, 2014. Accessed January 15, 2023. http://publication.pravo.gov.ru/Document/View/0001201501140003?rangeSize=20

———"Soglashenie mezhdu Pravitel'stvom Rossiyskoy Federacii i Pravitel'stvom Socialisticheskoy Respubliki V'etnam o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informacionnoy bezopasnosti [Agreement between the Government of the Russian Federation and the Government of the Socialist Republic of Vietnam on cooperation in the field of ensuring international information security]." September 6, 2018. Accessed January 15, 2023. http://publication.pravo.gov.ru/Document/View/0001201904290008?index=5&rangeSize=1

———"Soglashenie mezhdu Pravitel'stvom Rossiyskoy Federacii i Pravitel'stvom Turkmenistana o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informacionnoy bezopasnosti [Agreement between the Government of the Russian Federation and Turkmenistan on cooperation in providing international information security]." April 5, 2019. Accessed January 15, 2023. http://publication.pravo.gov.ru/Document/View/0001201906130020?index=2&rangeSize=1

———"Soglashenie o otrudnichestve gosudarstv – chlenov Organizacii Dogovora o kollektivnoy bezopasnosti v oblasti obespecheniya informacionnoy bezopasnosti

[Agreement on cooperation between the member states of the Collective Security Treaty Organization in the field of ensuring information security].” November 30, 2017. Accessed January 15, 2023. http://publication.pravo.gov.ru/Document/View/0001201904260001

Ministry of Telecommunications and Mass Media of the Russian Federation. Prikaz N 206 “Ob utverzhdenii plana deyatelnosti Ministerstva svyazi i massovyh kommunikaciy Rossiyskoy Federacii na period 2016-2021 godov [Decree No 206 “On approval of the activity plan of the Ministry of Telecommunications and Mass Media of the Russian Federation for the period of 2016-2021].” May 20, 2016. Accessed July 30, 2022. http://filearchive.cnews.ru/img/cnews/2016/06/29/16062016p24_5458vn.pdf

Moore, Daniel. *Offensive Cyber Operations: Understanding Intangible Warfare.* Oxford University Press. August 1, 2022. ISBN-10: 0197657559.

Mozur, Paul, Adam Satariano, Aaron Krolik, and Aliza Aufrichtig. “‘They Are Watching’: Inside Russia’s Vast Surveillance State.” *The New York Times.* September 22, 2022. Accessed February 15, 2023. https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html

Nacional’nyi Issledovatel’skiy Universitet “MEI” [National Research University “MEI”] “Prohozhdenie voennoi sluzhby v nauchnyh rotah [Military service in scientific companies].” March 11, 2022. Accessed July 30, 2022. https://mpei.ru/Structure/Universe/mei/Pages/company.aspx

Nakashima, Ellen. “Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes.” *Washington Post*. January 12, 2018. Accessed January 29, 2022. https://wapo.st/3IBY7Gk

Nakashima, Ellen. “The U.S. is urging a no vote on a Russian-led U.N. resolution calling for a global cybercrime treaty.” *The Washington Post*. November 16, 2019. Accessed August 1, 2022. https://wapo.st/3xr6yOr

National Institute of Standards and Technology (NIST) Glossary, s.v. “cyber attack.” Computer Security Resource Center (CSRC). Accessed February 5, 2022. https://csrc.nist.gov/glossary/term/Cyber_Attack

———s.v. “cyberspace capability.” Computer Security Resource Center (CSRC). Accessed February 5, 2022. https://csrc.nist.gov/glossary/term/cyberspace_capability

National Intelligence Council. “Foreign Threats to the 2020 US Federal Elections,” Intelligence Community Assessment 2020-00078D. March 10, 2021.

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

O'Donnell, Catherine. "New study quantifies use of social media in Arab Spring." University of Washington. September 12, 2011. Accessed July 28, 2022. https://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/

Oladimeji, Saheed and Sean M. Kerner. "SolarWinds hack explained: Everything you need to know." *TechTarget*. June 29, 2022. Accessed December 12, 2022. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Osborn, Andrew. "Bloggers who are changing the face of Russia as the Snow Revolution takes hold." *The Telegraph.* December 10, 2011. Accessed July 28, 2022. https://bit.ly/417SSWa

Osborne, Charlie. "Updated Kaseya ransomware attack FAQ: What we know now." *ZDNET*. July 23, 2021. Accessed January 29, 2022. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

OVD-Info.org. "Zakon o SMI-'inoagentah' nabiraet silu. Hronologiya [The law on media-'foreign agents' is gaining force. A chronology]." June 21, 2021. Accessed July 31, 2022. https://ovdinfo.org/articles/2021/06/21/zakon-o-smi-inoagentah-nabiraet-silu-hronologiya

Padilha, Luiz. "Brasil compra inovação russa para proteção de empresas contra ataques cibernéticos [Brazil buys Russian innovation to protect companies from cyberattacks]." *Defesa Aerea & Naval [Air and Sea Defense].* July 20, 2017. Accessed January 11, 2023. http://www.defesaaereanaval.com.br/brasil-compra-inovacao-russa-para-protecao-de-empresas-contra-ataques-ciberneticos/

Paganini, Pierluigi. "Krym: rossiyskaya kiberstrategiya voiny [Krimea: Russian cyber strategy or war]." *Den'* [*Day*]. March 27, 2014. Accessed July 30, 2022. https://day.kyiv.ua/ru/article/ekonomika/krym-rossiyskaya-kiberstrategiya-voyny

Peshkov, Aleksandr. "Shoigu: v MO RF sozdana Sistema prognozirovaniya vooruzhennyh konfliktov [Shoigu: a system for predicting armed conflicts has been created within Russia's Ministry of Defense]." *Zvezda TV* [*Star TV*]. December 16, 2019. Accessed July 30, 2022. https://tvzvezda.ru/news/201912161125-PViRZ.html

Petrov, Veniamin. "'Rosteh' zanyalsya parirovaniem kiberugroz ['Rosteh' engaged in parrying cyber threats]." *Izvestiya.* November 7, 2016. Accessed July 30, 2022. https://iz.ru/news/642771

Putin, Vladimir. "Vladimir Putin: Bezopasnost' v mire mozhno obespechit' tol'ko vmeste s Rossiey [Vladimir Putin: Security in the world can only be ensured together with Russia]. *Rossiyskaya Gazeta* [*The Russian Gazette*]. February 26, 2012.

Federal Issue №45(5718). Accessed January 2, 2023. https://rg.ru/2012/02/27/putin-politika.html

Qureshi, Waseem Ahmad. “Information Warfare, International Law, and the Changing Battlefield.” *Fordham International Law Journal.* Vol. 43:4 (2020). Accessed July 31, 2022. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2786&context=ilj

Radio Free Europe Radio Liberty. “Lenta.ru protiv uvolneniya glavnogo redaktora [Lenta.ru against the dismissal of the editor-in-chief].” March 13, 2014. Accessed July 31, 2022. https://www.rferl.org/a/25296359.html

RBC.ru. “Putin zapretil innostrannym kompaniyam issledovat’ teleauditoriyu v Rossii [Putin bans foreign companies from researching TV audiences in Russia].” July 4, 2016. Accessed July 31, 2022. https://www.rbc.ru/rbcfreenews/577a600e9a79471a6eb409f7

———“V 2015 godu telekanal Russia Today poluchit na 41% bolshe subsidiy [In 2015 TV channel Russia Today will receive 41% more government subsidies].” September 23, 2014. Accessed July 31, 2022. https://www.rbc.ru/politics/23/09/2014/5704227a9a794760d3d41a87

———“V.Putin utverdil ‘smertnuyu kazn’’ dlya SMI [V. Putin approved the ‘death penalty’ for the media].” April 8, 2013. Accessed July 31, 2022. https://www.rbc.ru/politics/08/04/2013/570406559a7947fcbd4478e1

Reporters without Borders. World Press Freedom Index. Accessed July 31, 2022. https://rsf.org/en/index?year=2015

Reuters. “Russian firm provides new internet connection to North Korea.” October 2, 2017. Accessed January 11, 2023. https://www.reuters.com/article/us-nkorea-internet-idUSKCN1C70D2

RIA Novosti [*RIA News*]. “Bolee 130 blogerov, priravnennyh k SMI, zaregistriroval Roskomnadzor [Roskomnadzor has registered more than 130 bloggers equated with mass media].” November 11, 2014. Accessed July 31, 2022. https://ria.ru/20141111/1032859288.html

———“Chislo polzovateley portala gosuslug priblizilos k sta millionam [The number of users of the government services portal approached one hundred million].” October 17, 2019. Accessed July 31, 2022. https://ria.ru/20191017/1559902373.html

———“Eksperty rasskazali o posledstviyah zakona ob ustoichivom Runete [Experts spoke about the consequences of the law on resilient Runet].” November 1, 2019. Accessed July 31, 2022. https://ria.ru/20191101/1560469853.html

———“Minoborony mozhet sozdat’ otdel’nyi rod voisk po bor’be s kiberugrozami [The Ministry of Defense may create a separate branch of the armed forces to combat cyber threats].” July 5, 2013. Accessed July 30, 2022. https://ria.ru/20130705/947802340.html

———“Shoigu: Minoborony mozhet nachat’ sozdavat’ nauchnye roty v universitetah [Shoigu: the Ministry of Defense may begin creating scientific companies at universities].” March 12, 2013. Accessed July 30, 2022. https://ria.ru/20130312/926805518.html

———“V irakskih shkolah nachnut izuchat’ russkiy yazyk [Iraqi schools to begin teaching Russian language].” November 14, 2017. Accessed July 31, 2022. https://ria.ru/20171114/1508770850.html

———“V shkolah Sirii vvedeno obyazatelnoye izuchenie russkogo yazyka [Compulsory study of the Russian language introduced in Syrian schools].” May 29, 2014. Accessed July 31, 2022. https://ria.ru/20140529/1009878505.html

Robertson, Jordan and Michael Riley. “Kaspersky Lab Has Been Working With Russian Intelligence.” *Bloomberg.* July 11, 2017. Accessed January 11, 2023. https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence

Rodriguez, Katitza and Karen Gullo. “Negotiations Over UN Cybercrime Treaty Under Way in New York, With EFF and Partners Urging Focus on Human Rights.” Electronic Frontier Foundation. March 3, 2022. Accessed August 1, 2022. https://www.eff.org/deeplinks/2022/03/negotiations-over-international-police-powers-agreement-must-keep-human-rights

Rogers, Zac. “The Promise of Strategic Gain in the Digital Information Age: What Happened?” *The Cyber Defense Review* Vol. 6, No. 1 (WINTER 2021), pp. 81-106.

Roskomsvoboda. “Monitoring Reyestra: Gosorgany udarno porabotali 23 fevralya (i +92 zaprewennyh IP [Registry Monitoring: State agencies worked hard on February 23 (and +92 banned IPs)].” February 27, 2013. Accessed July 31, 2022. https://roskomsvoboda.org/4445/

———“Reyestr zaprewennyh saitov [Registry of banned websites].” Accessed July 31, 2022. https://reestr.rublacklist.net/

Rostelecom. “Podvodnaya VOLS Kamchatka-Sahalin-Magadan [Underwater fiber optic communication line (FOCL) Kamchatka-Sakhalin-Mgadan].” Accessed July 31, 2022. https://www.company.rt.ru/projects/digital_economy_rf/focl/FarEast_FOCL/

Rostelekom-Solar. “AO ‘Kazahtelekom’ i Solar Security podpisali memorandum o partnerstve i vzaimodeistvii v oblasti kiberbezopasnosti [Kazakhtelecom and

Solar Security signed a memorandum of partnership and interaction in the field of cybersecurity].” April 27, 2017. Accessed January 11, 2023. https://rt-solar.ru/events/news/906/

Rothrock, Kevin. “Russia's Government Might Block Websites for Calls to Unsanctioned Rallies.” GlobalVoices.org. December 15, 2013. Accessed July 31, 2022. https://globalvoices.org/2013/12/15/russias-government-might-block-websites-for-calls-to-unsanctioned-rallies/

Russian Ministry of Finance. Annual information on the execution of the federal budget (data from January 1, 2006). June 27, 2022. Accessed July 31, 2022. https://minfin.gov.ru/ru/statistics/fedbud/execute/?id_65=80041-yezhegodnaya_informatsiya_ob_ispolnenii_federalnogo_byudzhetadannye_s_1_yanvarya_2006_g

Rustamova, Farida. “Budzhet gosudarstvennyh SMI v Rossii vyrastet na 2,5 milliarda rubley [The budget of state media in Russia will grow by 2.5 billion rubles].” *The BBC*. May 26, 2017. Accessed July 31, 2022. https://www.bbc.com/russian/news-40062877

Rutenberg, Jim. “RT, Sputnik and Russia’s New Theory of War.” *The New York Times*. September 13, 2017. Accessed July 31, 2022. https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html

Samarkina, Nina. “Strategii I Proekty Razvitiya Sovremennogo Oboronnogo Sectora RF [Strategies and Projects for the Development of a Modern Defense Sector of the Russian Federation].” *Vestnik RGGU*. Series: Political Science. History. International relations. Foreign area studies. Orientalism, 7, pages 21 – 28. (2014). Accessed July 30, 2022. https://elibrary.ru/item.asp?id=21769543

Samigullina, Alya and Natalya Kuklina. “Eto propaganda v tradicii Sovetskogo Souza [This is propaganda in the tradition of the Soviet Union].” *Gazeta.ru.* August 13, 2008. Accessed July 28, 2022. https://www.gazeta.ru/politics/2008/08/12_a_2809214.shtml?updated

Sanders, Robert. “The U.S. government no longer controls the internet.” *Business Insider*. October 4, 2016. Accessed July 30, 2022. https://www.businessinsider.com/the-us-government-no-longer-controls-the-internet-2016-10

Sauer, Pjotr. “Putin ally Yevgeny Prigozhin admits founding Wagner mercenary group.” *The Guardian*. September 26, 2022. Accessed January 15, 2023. https://www.theguardian.com/world/2022/sep/26/putin-ally-yevgeny-prigozhin-admits-founding-wagner-mercenary-group

Schelling, Thomas. *The Strategy of Conflict.* Harvard University Press. 1981. ISBN 9780674840317.

Shakirov, Oleg I. "Kto pridet s kibermechem: podhody Rossii I SsHA k sderzhivaniyu v kiberprostranstve [Whoever Comes with a Cyber Sword: Russian and U.S. Approaches to Deterrence in Cyberspace]." *Journal of International Analytics*. 2020;11(4):147-170. Accessed Aug 15, 2022. https://www.interanalytics.org/jour/article/view/326

Sharikov, Pavel. "Global Cybersecurity at Stake Amid US and Russia's Disagreements." Italian Institute for International Political Studies. September 7, 2021. Accessed July 31, 2022. https://www.ispionline.it/en/pubblicazione/global-cybersecurity-stake-amid-us-and-russias-disagreements-31435

———"Understanding the Russian Approach to Information Security," European Leadership Network, January 16, 2018. Accessed July 28, 2022. https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/

Shvec, Yana V. "Vliyanie televidiniya na informacionnoe prostranstvo sovremennoy Rossii [The influence of television on the information space of modern Russia]." *Bulletin of the Volga Region Institute of Administration*. 2018. Vol.18 No.2. Accessed July 31, 2022. https://cyberleninka.ru/article/n/vliyanie-televideniya-na-informatsionnoe-prostranstvo-sovremennoy-rossii

Skolkovo Foundation. "Klastery 'Skolkovo' [The Clusters of 'Skolkovo']." Accessed July 30, 2022. https://sk.ru/foundation/clusters/itc/

———"The Clusters." Accessed July 30, 2022. https://old.sk.ru/foundation/about/p/clusters.aspx

Smith, M.L.R. "Strategic Theory: What it is…and just as importantly, what it isn't." *E-International Relations.* April 28, 2011. ISSN 2053-8626. Accessed August 17, 2022. https://bit.ly/3EHRSi3

Sokolov, Kirill. "Rassledovanie RBK: kak iz 'fabriki trolley' vyrosla 'fabrika media' [RBC investigation: how a 'media factory' grew out of a 'troll factory']." *RBC.ru*. March 24, 2017. Accessed July 31, 2022. https://www.rbc.ru/technology_and_media/24/03/2017/58d106b09a794710fa8934ac

Soldatkin, Vladimir and Steve Holland. "Far apart at first summit, Biden and Putin agree to steps on cybersecurity, arms control." Reuters. June 16, 2021. Accessed February 1, 2022. https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/

Soldatov, Andrei and Irina Borogan. "Russia's Approach to Cyber: The Best Defence is a Good Offence." European Union Institute for Security Studies (EUISS). 2018. Accessed July 30, 2022. https://www.jstor.org/stable/resrep21140.5

———“The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries.” *Public Affairs*, 2015.

Soldaty RF [*Soldiers RF*]. “Rossiya: odna armiya i tri mneniya [Russia: One Army and Three Opinions].” May 3, 2012. Accessed April 9, 2022. https://www.soldati-russian.ru/news/rossija_odna_armija_i_tri_mnenija/2012-03-05-1408

Soshnikov, Andrei. “Stolica politicheskogo trollinga [The capital of political trolling].” *MR7.ru*. March 11, 2015. Accessed July 31, 2022. https://mr-7.ru/articles/112478/

Soshnikov, Andrey. “Internet-trolli iz Olgino zagovorili na angliyskom i ukrainskom [Internet trolls from Olgino started to speak in English and Ukrainian].” *MR7.ru*. May 30, 2014. Accessed July 31, 2022. https://mr-7.ru/articles/102680/

Sostav.ru. “Dolya rossiyskogo kino v obwem prokate vpervye prevysila dopandemiynyi pokazatel [The share of Russian cinema in general distribution for the first time exceeded the pre-pandemic figures].” July 19, 2021. Accessed July 31, 2022. https://www.sostav.ru/publication/rossijskoe-kino-rost-prokata-49480.html

Surovikin, Sergey. V., “Forms for Employing and Organizing Command and Control of a Joint Troop (Force) Grouping in the Theater of Military Activity,” *Vestnik Akademii Voennykh Nauk* [*Bulletin of the Academy of Military Sciences*], Vol. 1, No.46, 2014.

Sutyagin, Igor. “Russian Forces in Ukraine.” Royal United Services Institute. Briefing Paper. March 2015. Accessed February 13, 2023. https://rusi.org/explore-our-research/publications/briefing-papers/russian-forces-ukraine

TAdviser. “Internet-trafik RF pod control’ [RF internet-traffic under control].” Accessed July 30, 2022. https://bit.ly/3S1A5Yn

———“Nacionalny centr upravleniya oboronoi Rossii (NCUO RF) [National Defense Management Center of Russia (NDCC RF)].” Accessed July 30, 2022. https://bit.ly/3HX8vXw

Tashev, Blagovest, Michael Purcell, and Brian McLaughlin. “Russia’s Information Warfare Exploring the Cognitive Dimension.” *MCU Journal* vol. 10, No.2. Fall 2019.

TASS. “Chislo pol’zovateley interneta v Rossii dostiglo 124 mln [The number of Internet users in Russia reached 124 million].” October 19, 2021. Accessed March 7, 2023. https://tass.ru/obschestvo/12698757

———“Putin podpisal zakon o zaprete mata v kino, spektaklyah I na koncertah [Putin signed a law banning obscenities in movies, performances and concerts].” May 5, 2014. Accessed July 31, 2022. https://tass.ru/kultura/1166943

———"'Rostelekom' vlozhil bolee 10 mlrd rublei v liniyu svyazi ot Ekaterinburga do Saleharda [Rostelecom invested more than 10 billion rubles in a communication line from Yekaterinburg to Salekhard]." April 15, 2014. Accessed July 31, 2022. https://tass.ru/ekonomika/1121596/amp

———"Russia initiates its draft of int'l convention on countering cybercrime." July 27, 2021. Accessed August 1, 2022. https://tass.com/politics/1318319

———"V dvuh Kubinskih shkolah nachnut prepodavat' russkiy yazyk [Russian language will be taught in two Cuban schools]." February 15, 2018. Accessed July 31, 2022. https://tass.ru/obschestvo/4959319

The Federal Council, Russian Federation. "Koncepciya strategii kiberbezopastnosti Rossiyskoy Federacii [The Russian Federation Cybersecurity Strategy Concept]." January 10, 2014. Accessed January 29, 2023. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

The White House, United States. "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government." April 15, 2021. Accessed December 12, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

———"FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government." April 15, 2021. Accessed February 5, 2023. https://bit.ly/3IdqskP

———Office of the Press Secretary. "Joint Statement on the Inaugural Meeting of the U.S.-Russia Bilateral Presidential Commission Working Group on Threats to and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security." Press release. National Archives and Records Administration. November 22, 2013. Accessed March 5, 2023. https://obamawhitehouse.archives.gov/the-press-office/2013/11/22/joint-statement-inaugural-meeting-us-russia-bilateral-presidential-commi

Thomas, Timothy L. "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations." *Journal of Slavic Military Studies*, 1998, Vol.11, No.1, pp. 40-62. Accessed August 14, 2022. https://community.apan.org/cfs-file/__key/docpreview-s/00-00-08-56-53/1998_2D00_03_2D00_01-Dialectical-Versus-Empirical-Thinking-_2800_Thomas_2900_.pdf

Trunina, Anna and Andrey Zaharov. "'Fabrika trolley' pereehala v 'Lahtu-2' [Troll factory moved to Lakhta-2]." *RBC.ru.* December 30, 2017. Accessed July 31, 2022. https://www.rbc.ru/business/30/12/2017/5a465d969a79472a87a3c920

U.S. Cybersecurity & Infrastructure Security Agency. Alert (AA21-116A) "Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders." April 26, 2021. Accessed December 23, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa21-116a

———Alert (AA22-110A) "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." April 20, 2022. Last revised: May 9, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

U.S. Department of Justice Office of Public Affairs. "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election." Press Release. July 13, 2018. Accessed February 5, 2023. https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

———"U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts." Press release. March 15, 2017. Accessed July 30, 2022. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

———United States of America v. Internet Research Agency LLC. 18 U.S.C. §§ 2, 371, 1349, 1028A. Case 1:18-cr-00032-DLF. (2018). Accessed July 31, 2022. https://www.justice.gov/file/1035477/download

U.S. Department of State Global Engagement Center. "Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem." Special Report. January 2022. Accessed July 31, 2022. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf

U.S. Department of the Treasury. "Treasury Sanctions Russia with Sweeping New Sanctions Authority." April 15, 2021. Accessed February 5, 2023. https://home.treasury.gov/news/press-releases/jy0127

U.S. Secretary of Defense. *Strategic Communication and Information Operations in the DOD*. Memorandum. January 25, 2011. Accessed July 30, 2022. http://www.ecrow.org/assets/osd%2012401-10.pdf

United Nations General Assembly. "Advancing responsible State behaviour in cyberspace in the context of international security." A/C.1/73/L.37. October 18, 2018. Accessed August 1, 2022. https://bit.ly/3YDK74w

———"Convention on countering the use of information and communications technologies for criminal purposes." Articles 19, 33. June 29, 2021. Accessed August 1, 2022. https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf

———"Countering the use of information and communications technologies for criminal purposes." A/RES/73/187. 2018. New York. Accessed August 1, 2022. https://digitallibrary.un.org/record/1660536?ln=en

———"Countering the use of information and communications technologies for criminal purposes." A/C.3/74/L.11/Rev.1. November 5, 2019. Accessed August 1, 2022. https://undocs.org/A/C.3/72/12

———"Developments in the field of information and telecommunications in the context of international security." A/C.1/73/L.27/Rev.1. October 29, 2018. New York. Accessed August 1, 2022. https://bit.ly/3S3Bg9R

———"Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." A/66/359. Accessed July 31, 2022. https://www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E

United Nations. UN E-Government Survey 2018. Accessed July 31, 2022. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018

Universal Rights Group. "Report on the 74th session of the Third Committee of the UN General Assembly." November 25, 2019. Accessed August 1, 2022. https://www.universal-rights.org/blog/report-on-the-74th-session-of-the-third-committee-of-the-un-general-assembly/

Vedomosti. "'Interfaks' soobschil o planah Minfina vydelit 'Skolkovo' ewe 45 milliardov rublei [Interfax announced the plans of the Ministry of Finance to allocate another 45 billion rubles to Skolkovo]." September 7, 2018. Accessed July 30, 2022. https://www.vedomosti.ru/economics/news/2018/09/07/780265-skolkovo

Volchek, Dmitry. "Bezumie, kremlevskih trollei [Madness of Kremlin's trolls]." *Radio Svoboda* [*Radio Freedom*]. March 15, 2015. Accessed July 31, 2022. https://www.svoboda.org/a/26913247.html

Volkov, Denis and Stepan Goncharov. "Rossiyskiy Media Landshaft – 2017 [Russian Media Landscape – 2017]." Levada-Centr [Levada Center]. August 22, 2017. Accessed March 7, 2023. https://www.levada.ru/2017/08/22/16440/

Volkov, Denis, Stepan Goncharov, Aleksandra Paramonova, and Denis Leven. "Rossiyskiy Media Landshaft – 2021 [Russian Media Landscape – 2021]." Levada-Centr [Levada Center]. August 5, 2021. Accessed March 7, 2023. https://www.levada.ru/2021/08/05/rossijskij-medialandshaft-2021/

Vorontsova, L. V. and Frolov, D. B. *Istoriya i Sovremennost' Informatsionnovo Protivoborstva* [*History and Modernity of Information Confrontation*], Goryachaya liniya-Telekom, 2006. ISBN 5-93517-283-6.

Weedon, Jen. "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine." FireEye. 2015. In Kenneth Geers (ed.).

Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO CCD COE Publications. ISBN 978-9949-9544-5-2.

Yandex. "Razvitie interneta v regionah Rossii [Internet access in the regions of Russia]." 2012. Accessed July 31, 2022. https://yandex.ru/company/researches/2012/internet_regions_2012

Yarger, Harry R. *Strategic Theory for the 21st Century: The Little Book on Big Strategy.* U.S. Army War College Press, 2006. Accessed December 14, 2022. https://press.armywarcollege.edu/monographs/723

Zabierek, Laudern, Christie Lawrence, Miles Neumann and Pavel Sharikov. "US-Russian Contention in Cyberspace Are 'Rules of the Road' Necessary or Possible?" Belfer Center for Science and International Affairs, Harvard Kennedy School. June 2021. Accessed August 18, 2022. https://www.russiamatters.org/analysis/us-russian-contention-cyberspace-are-rules-road-necessary-or-possible

Zaitsev, Anatoly. "Partizanskimi Metodami: Sovremennaya armiya doljna umet' voevat' bez linii fronta [Partisan Methods: Modern army must be able to fight without the frontline]." *Voenno-Promyshlennyi Kur'er* [*The Military-Industrial Courier*]. September 1, 2014. Published in print in issue No.32 (550), September 3, 2014. Accessed July 30, 2022. https://vpk-news.ru/articles/21649