Russia's Cyber Operations

A Threat to American National Security

Dave Aitel, Sophia d'Antoine, Thomas Garwin, Ian Roos, Nicholas Rostow, Justin Sherman, and Abraham Wagner

MARGIN RESEARCH

The research described in this report was sponsored by the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR00112190088. The views expressed are those of the authors, and do not necessarily reflect the views or opinions of the U.S. Government.

www.margin.re

Contents

Foreword and Acknowledgements

What began as a research project at the Advanced Research Projects Agency (ARPA) in the 1960s evolved into a communications and information technology revolution never anticipated. These new technologies gave rise to the most significant paradigm change since the invention moveable type in the 15th century. Now almost all communications and information operations now use the Internet infrastructure. All major sectors—national security, finance, utilities—depend on this critically important infrastructure.

At the same time, dependence on this infrastructure makes users vulnerable to attack. While the original ARPA effort was an experiment in networking scientists, it did not take security into account. The foundation of ARPAnet and the Internet has remained insecure and prone to hostile attacks of all kinds even as the Internet has developed almost without known or knowable limits.

The Internet and information technologies created a new technological context for espionage, warfare, and crime. As a result, cyber espionage and cyber warfare have become major national security problems. Here the Defense Department and Intelligence Community recognize cyber warfare as a major threat area and the cyber landscape as a domain for activity equal in importance and perhaps more important than land, sea, air, and space.

The most significant cyber threats now come from four states—Russia, China, North Korea, and Iran. The research team has considered the ways in which each of these states recruit skilled personnel, organize their potentially malicious activities, and undertake specific cyber operations. An increasing number of hostile Russian attacks and the way Russia conducts its war in Ukraine demonstrate the seriousness of the evolving threat. Russia's interest in the information area is generations old. The present technological context has led Russia greatly to expand its cyber capabilities, especially with respect to espionage, intelligence collection, and cyber warfare.

This threat has received increasing notice and discussion in the open literature although data supporting Russia's malicious cyber operations are limited. The present analysis is based on a technical effort using open-source material generated by Russian operations and code artifacts inserted into software, exploring the cyber ecosystem, rather than simply observing the aftermath of hostile cyber activities, with a view toward actually solving important parts of the cybersecurity problem.

This study effort was made possible with support from the Defense Advanced Research Projects Agency (DARPA). The study team has benefited greatly from discussions with personnel from U.S. Government agencies and offices, as well as former officials and other experts. In particular, Alexei Bulazel, Daniel Gallington, Anthony Cordesman, and J.D. Work have been extraordinarily helpful throughout this process.

Also supporting the work have been several research assistants, currently graduate and law students at Harvard University and New York University (NYU) School of Law. The views expressed do not reflect the views of any organization or the U.S. Government.

Dave Aitel
Sophia d'Antoine
Thomas Garwin
Ian Roos
Nicholas Rostow
Justin Sherman
Abraham Wagner

December 1, 2022

Executive Summary

A 1960s research project at the Advanced Research Projects Agency (ARPA) began a technology revolution never anticipated and the most significant paradigm change since the invention of movable type. Today, most communications and information operations take place on systems connected to the Internet infrastructure. Dependence on this infrastructure makes users vulnerable to hostile attacks by criminal enterprises and foreign intelligence and military organizations. Russia stands out as one of the most significant threats, having greatly expanded its cyber capabilities with respect to intelligence collection, espionage, and cyber warfare as it engages in these activities on a continuing basis.

Russia views cyber differently than its western counterparts. Russia's leadership sees itself as engaged in an ongoing, existential struggle in every realm, including the information space. Moscow views the Internet as a threat to regime security and a weapon to be used against Russia's enemies and does not use the term "cyber" or "cyber warfare" except in reference to Western concepts, preferring to see cyber operations in the broader framework of information security and information warfare. This holistic concept includes computer network operations, electronic warfare, psychological operations, and information operations. Consistent with Soviet notions of combating ongoing threats from abroad and within, the present Russian regime views the struggle over "information space" as unending.

Offensive cyber operations play a large and increasing role in Russian military operations and in Russia's strategic deterrence framework. While, for structural and doctrinal reasons, the Russian military and intelligence services were slow to embrace cyber operations, the government now plans to bolster the offensive and defensive cyber capabilities of the armed forces and other security institutions. As Russia's cyber operations grow at a pace and on a scale well beyond what has been widely reported, there is a great opportunity to use open-source information and data to understand the nature of these operations and the threat they constitute.

A central objective of the DARPA Social Cyber program is to utilize a comprehensive approach to understand the culture and the anthropology of the software development process with regard to malicious code and open-source software (OSS). Russia's cyber threats and operational components have resisted identification by traditional intelligence methods: the source data is not part of the usual collection regime, and the AI analytical tools, such as those utilized for this study, rely on a major software development effort integral to the DARPA program. The present analysis looks at how malicious code is distributed; AI tools search open-source source materials and extract and analyze the data obtained.

This study of Russia's cyber operations, hacker community, and open-source code yields a number of key findings:

- **The Russian government sees the Internet both as a threat to regime security and a weapon to be used against its enemies.** It generally does not use "cyber" in its

doctrines, policy documents, and debates except in reference to Western concepts. Instead, Moscow orients much of its thinking around the notion of "information security" (*informatisonnaya bezopastnost*)—a much broader concept that includes technical elements like encryption but also includes the state's ability to control and shape the overall information space. Hence, Russian actors often carry out cyber and information operations in tandem.

- **Russia's cyber operations fit under the "active measures" (*aktivnye meropriyatiya)* umbrella.** For more than a century, Russia has used forgeries, disinformation, and falsehood-propagation alongside assassinations, sponsorship of coups, and other covert activities to project influence and undermine Russia's perceived enemies. While the Internet and other technological advances brought profound changes, Russian cyber and information operations still emphasize deniability and blur the lines between public diplomacy and propaganda—key features of decades-old active measures.
- **Russian military doctrine increasingly emphasizes cyber operations to project power and, conversely, the threat of foreign cyber and information operations to Russia.** The 2008 Russia-Georgia War catalyzed Russia's creation of an official offensive and defensive cyber operations unit; its *2010 Military Doctrine* stated that "information warfare" was playing a greater role in military conflict. Since Putin came to power in December 1999, Moscow has carried out cyber operations before initiating armed military conflict to increase confusion, contribute to the "fog of war," and assert control over the information environment.
- **The Russian government uses a network of actors to support its capability development, talent cultivation, and cyber operations.** This network includes government cyber units, principally in the Federal Security Service (FSB), Foreign Intelligence Service (SVR), and military intelligence agency (GRU). It also includes cybercriminals and individual developers recruited by the government, "entrepreneurial" hackers approaching the state, and government-created front companies. The government also leverages hackers with mafia-style familial connections to the security services, encourages patriotic hackers, weaponizes private military companies (PMCs), and uses private-sector conferences and gatherings to recruit talent. Understanding Russia's cyber power requires understanding the numerous actors, including non-state actors, in this complex ecosystem.
- **Companies like Positive Technologies, SecurityCode, Kaspersky, Infotecs, and Sberbank Technology play central roles in the Russian cybersecurity ecosystem.** Positive Technologies has been sanctioned by the U.S. government for supporting Russian cyber operations and hosting events that the FSB and GRU use to recruit hackers. Infotecs is on the U.S. Entity List for enabling the malicious activity of Russian cyber actors. Their support for the state might be defensive or offensive; they may also simply act as vehicles through which Russian cyber talent is trained and Russian code is developed.

- **Russia's "brain drain" remains a persistent problem.** It will likely weaken Russia's ability to maintain an up-to-date, innovative technology sector and a cyber talent pool, at least in the near term. Nonetheless, Russian universities continue to launch cybersecurity programs, the Russian military now has several, and the government remains intent on developing Russian domestic technology and influencing the global software base.
- **Russia has demonstrated a wide range of cyber capabilities.** These include phishing, DDoS attacks, password brute-force algorithms, ransomware, and malware to shut down electrical grid Supervisory Control and Data Acquisition (SCADA) systems. This enables Russia to inflict enormous damage on the financial sector and to break into systems abroad for surveillance purposes, ranging from hacks of the Georgian Ministry of Defense to the widespread SolarWinds espionage campaign against the U.S. Moscow builds many of these capabilities in-house and has also turned to programmers at companies and cybercriminals to develop capabilities.
- **Russia has expanded its focus on open-source software as a replacement for Western technology and to expand its global tech footprint—raising security risks for U.S. software.** The Astra Linux operating system is key to Russia's domestic tech development efforts, and since February 2022, Moscow has accelerated its efforts to remove Western software and hardware, replacing it with Russian technology. Lately, Russian companies have been discussing overseas expansion via software products; Russian developers are working on building an entire Russian technology stack based around Astra Linux; and the Russian government has been purchasing Chinese computers, requiring that Astra Linux is installed on those systems.
- **The Margin Research team has developed a set of artificial intelligence (AI) tools to assist in the analysis of Russia's cyber operations.** This includes individuals engaged in open-source development in Russia, China, North Korea, and Iran in addition to the institutions and agencies supporting them. This extensive data collection and analysis on open-source software contributors enables specific code contributions within the Linux Kernel and those behind them. It has also enabled analysis of other Russian code outside Linux, such as the software development kit (SDK) made by Pushwoosh, a Russian organization falsely presenting as U.S.-based.

The analysis of open-source software, social media, and those that create it is a useful way to identify suspicious cyber activity and malicious cyber operations, and the novel AI techniques developed by Margin Research support an analysis pipeline of Russian cyber operations and the actors involved. While prior analyses lacked the tools necessary to uncover such behavior, they also did not have access to the large body of data collected in the present effort. Going forward, it is essential to continue this critical line of research into the Russian cyber ecosystem, an area of increasing significance to U.S. national security.

1. Introduction

From the way Russian theorists define cyber warfare to how the Russian government employs its cyber capabilities, Russia views cyber differently than its western counterparts. For some time, the Russian leadership has seen itself as engaged in an ongoing, existential struggle against internal and external forces seeking to challenge its security using information and information technologies. The Russian government translates that perceived threat into a threat to the regime. At the same time, the government sees the Internet and the free flow of information it engenders as an opportunity.

Russian military theorists avoid using the terms "cyber" or "cyber warfare"; instead, they conceptualize cyber operations in the broader framework of information warfare. This approach involves a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations. Consistent with Soviet notions of combating ongoing threats from abroad and within, Russia views the struggle over "information space" as constant and unending. This fact, and it is a fact, suggests that the Russian leadership will have a relatively low bar for employing cyber in ways that U.S. leadership will see as offensive, involving conflict escalation *per se*.

Offensive cyber operations play a large and increasing role in conventional Russian military operations. They may play a future role with respect to Russian strategic deterrence. While the Russian military and intelligence services have been slow to embrace cyber operations for structural and doctrinal reasons, there are increasing signs that the government plans to bolster the offensive and defensive cyber capabilities of the armed forces and other security institutions.[1]

Along with the Russian military and its contractors, hacktivists and cybercriminal syndicates have been a central feature of Russian offensive cyber operations. They give Russia

[1] During operations in Georgia and Ukraine, Russia appeared to employ cyber as a conventional force enabler. The Georgia and Ukraine conflicts also provided opportunities for Russia to refine their cyber warfare techniques and procedures and to demonstrate their capabilities to the world. These demonstrations later may serve as a basis to signal or deter Russia's adversaries. See Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington: Georgetown University Press, 2020); Justin Sherman, "Digital Active Measures: Historical Roots of Contemporary Russian Cyber and Information Operations," *Georgetown Security Studies Review* (April 2, 2022); Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington: Center for Naval Analysis, March 2017); and Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019**)**.

easily mobilized, anonymous, and deniable cyber assets and actors. At the same time, while Russia has utilized hackers and criminal networks in the past, contemporary evidence suggests that there is a high degree of engagement between Russian government agencies and criminals, independent hackers, and other non-state actors in the vast Russian cyber web.

Russia's Model for Cybersecurity

The Russian model for malicious cyber activity includes components of the intelligence service, such as the Federal Security Service (FSB) and the Russian Federation's Main Intelligence Directorate of the General Staff (GRU), or military intelligence agency, and "external" contract activity, such as the Internet Research Agency (IRA). To some extent, this is similar to the model employed by the United States, where cyber activities are undertaken by the intelligence agencies, chiefly NSA, CYBERCOM, and CIA, and a number of external support contractors. In other ways, though, it is different given the corruption, lack of accountable oversight, and illicit financing behind organizations like the IRA. Other commercial operations within Russia, such as cybersecurity firms Positive Technologies and Kaspersky, are known to support Russian government requirements and engage in the international sale of commercial security products.

Russia's IRA, based in St. Petersburg, has received substantial funding from Russian oligarch Yevgeniy Viktorovich Prigozhin and companies he controls, which include Concord Management and Consulting LLC, Concord Catering, and the Wagner Group.[2] Prigozhin is widely reported to have strong ties to Russian President Vladimir Putin. Whether the Russian government or its military and intelligence services directly fund the IRA is not publicly known.[3]

As early as 2014, the IRA sent employees to the United States on an intelligence gathering mission and later used accounts on social media and interest groups to sow discord in the U.S. political system through what it termed "information warfare." The campaign evolved from a generalized program designed in 2014 and 2015 to undermine the U.S. electoral system to a targeted operation that by early 2016 favored candidate Donald Trump and disparaged candidate Hillary Clinton. In January 2018, Twitter announced that it had identified 3,814 IRA-controlled Twitter accounts and notified approximately 1.4 million people Twitter believed may have been in contact with an IRA-controlled account.

At least since the 2016 election cycle, cyber units in the GRU have hacked the computers and email accounts of organizations, employees, and volunteers supporting the Hillary Clinton presidential campaign, including its campaign chairman John Podesta.[4] The GRU hacked into the

[2] See "Russia's Wagner Group opens defence tech centre in St Petersburg," *The Guardian* (November 4, 2022)

[3] There has been extensive investigation of the IRA by the team working for Special Counsel Mueller. Several U.S. Attorneys in different districts have filed indictments against them. See Abraham Wagner and Nicholas Rostow, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2020), 758-789. For the full report, see Special Counsel Robert S. Mueller, III, *Report on the Investigation into Russian Election Interference in the 2016 Presidential Election: Submitted to the Attorney General Pursuant to 28 CFR §600.8(c)* (March 2019).

[4] Military Unit 74455 is a related GRU unit with multiple departments that engaged in cyber operations. Unit 74455 assisted in the release of documents stolen by Unit 26165, the promotion of those releases,

computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC), targeting hundreds of email accounts.

In total, the GRU stole hundreds of thousands of documents from the compromised email accounts and networks. The GRU later released stolen Clinton Campaign and DNC documents through online personas, including "DCLeaks" and "Guccifer 2.0," and via WikiLeaks. The release of the documents was designed and timed to interfere with the 2016 U.S. presidential election.

Two military units of the GRU, for example, carried out the computer intrusions into the Clinton Campaign, DNC, and DCCC: Military Units 26165 and 74455. Military Unit 26165 is a GRU cyber unit dedicated to targeting military, political, governmental, and non-governmental organizations outside Russia, including in the United States.[5] The unit was sub-divided into departments with different specialties. For example, one department developed specialized malicious software (malware), while another department conducted large-scale spearphishing campaigns.[6]

GRU officers gained access to the DNC network via a virtual private network (VPN) connection between the DCCC and DNC networks. Unit 26165 compromised more than 30 computers on the DNC network, including the DNC mail server and shared file server and implanted on the DCCC and DNC networks two types of customized malware, including one known as "X-Agent" and "X-Tunnel," Mimikatz, a credential-harvesting tool, and rar.exe, a tool used in these intrusions to compile and compress materials for exfiltration. X-Agent was a multi-function hacking tool that allowed Unit 26165 to log keystrokes, take screenshots, and gather other data about the infected computers (e.g., file directories and operating systems).

X-Tunnel was a hacking tool that created an encrypted connection between the victim DCCC/DNC computers and GRU-controlled computers that was capable of large-scale data

---

and the publication of anti-Clinton content on social media accounts operated by the GRU. Officers from Unit 74455 separately hacked computers belonging to state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.

[5] The government charged 12 GRU officers for crimes arising from the hacking of these computers, principally with conspiring to commit computer intrusion s, in violation of 18 U.S.C. §§ 1030 and 371. See *United States v. Netyksho,* (18-cr-215) (D.D.C. July 13, 2018). Separately in October 2018 a grand jury sitting in the Western District of Pennsylvania returned an indictment charging certain members of Unit 26165 with hacking the U.S. Anti-Doping Agency, the World Anti-Doping Agency, and other international sport associations. *United States v. Morenets*, (18-cr-263) (DC WDPA, 2018).

[6] Military Unit 74455 is a related GRU unit with multiple departments that engaged in cyber operations. Unit 74455 assisted in the release of documents stolen by Unit 26165, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU. Officers from Unit 74455 separately hacked computers belonging to state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.

transfers. GRU officers then used X-Tunnel to exfiltrate stolen data from the victim computers. To operate X-Agent and X-Tunnel on the DCCC and DNC networks, Unit 26165 officers set up a group of computers outside those networks to communicate with the implanted malware.

The first set of GRU-controlled computers, known by the GRU as "middle servers," sent and received messages to and from malware on the DNC/DCCC networks. The middle servers, in turn, relayed messages to a second set of GRU-controlled computers, labeled internally by the GRU as an "AMS Panel." The AMS Panel served as a nerve center through which GRU officers monitored and directed the malware's operations on the DNC/DCCC networks.

The Arizona-based AMS Panel also stored thousands of files containing keylogging sessions captured through X-Agent. These sessions were captured as GRU officers monitored DCCC and DNC employees' work on infected computers. Data captured in these key logging sessions included passwords, internal communications between employees, banking information, and sensitive personal information.

Russia's Cyber Ecosystem

While the Russian government cultivates an ecosystem in which cybercrime and "patriotic hacking" thrives, it does not exercise total, constant control over every cyber and information actor in Russia. Instead, Moscow supports some actors regularly and others as needed. The cyber and information actors at Moscow's disposal include:

- Government cyber units, principally in the FSB, SVR, and GRU;
- Cybercriminals and individuals actively recruited by the government;
- "Entrepreneurial" hackers and developers to whom or which the government provides incentives to develop their own cyber and information capabilities and services for Russian intelligence community use;
- Hackers with mafia-style familial connections to the security services;
- Cyber and information front companies, set up and run by the government;
- Academic institutions and think tanks that help the government cultivate and recruit cyber and information talent and promote its "information security" vision;
- Patriotic hackers encouraged by the government; and
- Private military companies that offer, or could develop, cyber and information capabilities.

The DARPA Social Cyber Initiative

A central objective of the DARPA Social Cyber program is to utilize a holistic approach to understand the culture and the anthropology of the software development process with regard to malicious code and open-source software (OSS). As part of this effort, the research team has analyzed the various "models" or ways in which personnel who engage in the development of malicious code and OSS projects are recruited and trained in Russia, China, North Korea, and Iran.

Of particular importance at present are Russia's rapidly growing cyber operations. They have progressed quickly and on a scale well beyond what has been widely reported within the U.S. national security community. The Russian "model" goes beyond malicious and offensive cyber operations undertaken in the past by the military, the GRU, the SVR, and the FSB and has now greatly expanded into outsourced commercial operations, incorporating a far larger talent pool. The expanded scope of cyber operations includes theft and exploitation of data for national security purposes and the development of exploits and other malicious cyber tools supporting an expanded cyber warfare capability and agenda.

This activity represents a serious national security concern worthy of far greater attention in both the policy and technical domains. Current research has found that these cyber threats are far more extensive than previously supposed. The nature of the threat and operational components have resisted identification by traditional intelligence methods, as the source data is not what is part of the usual collection regime, and the AI analytical tools, such as those utilized here, rely on a major software development effort that has been an integral part of the DARPA program.

The present analysis considers the operational mechanisms by which such malicious code is distributed by these actors or their surrogates.[7] In each case the effort utilizes a search of open-source source materials, with native-language speakers as part of the effort as well as a set of software tools to extract and analyze the available data. The research team has worked to identify specific code coming from China, as well as the other hostile powers, within the Linux kernel and elsewhere which is the result of these activities. The effort also aims to tie specific individual actors to the code generated.

[7] An important objective of the DARPA SocialCyber program aims to understand the culture and the anthropology of the software development process with regard to malicious code and OSS projects, considering the "models" or ways in which personnel who engage in the development of malicious code and OSS projects are recruited and trained.

2. Evolution of Russia's Cyber Strategy

The Russian government does not view the Internet in the same way as many others do, as a liberalizing force, free from state control. In fact, Russian doctrine does not make reference to "cyber" as its own function, domain, or concept except in reference to western documents and thinking, such as the Defense Department's conceptualization of "cyberspace" as the fifth domain of warfare.[8] Instead, Moscow orients much of its thinking around the notion of "information security" (*informatisonnaya bezopastnost*). This term is used in the West, generally, in reference to the confidentiality, availability, and integrity of systems, networks, and data—roughly synonymously with "cybersecurity."

In Russian government documents, "information security" is a much broader concept, referring to the state's ability to control and shape the information space and the creation, processing, and dissemination of information within it. For example, the 2000 *Information Security Doctrine of the Russian Federation*, signed shortly after Vladimir Putin first became President—when he still claimed Russia aimed to become a fully democratic European state—defined information security as "the state of the protection of [the Russian Federation's] national interest in the information sphere, as determined by the overall balanced interests at the level of the individual, society, and the state."[9]

Information security includes technical elements like encryption but also encompasses political, social, and informational concepts like public opinion and regime stability. This broad conceptualization, among other drivers of Russian thinking, is reflected in the fact that Russian state and state-backed actors often carry out cyber and information operations in tandem.

A recent analysis of China's cyber operations found that Beijing has "always understood the importance of controlling information for domestic control and in competition and conflict."[10] It also underscored that China's objective in cyberspace is to control *information*, rather than to control cyberspace.[11] Moscow likewise views cyber operations as a way to reinforce information control, whether through disruptive operations launched against foreign media websites during conflict or espionage campaigns used to study a foreign country and then exploit its population's divisions.

---

[8] *Department of Defense Cyber Strategy 2018*. See also, Valeriy Akimenko and Keir Giles, "Russia's Cyber and Information Warfare," *Asia Policy* (2020): 67-75, 68. See also, Department of Defense, *National Defense Strategy 2022* (March 28, 2022).

[9] Russian Government, *Information Security Doctrine of the Russian Federation* (September 9, 2000), p. 1.

[10] Dave Aitel, et al., *China's Cyber Operations: The Rising Threat to American Security* (New York: Margin Research, 2022), Report for Defense Advanced Research Projects Agency, viii.

[11] *Ibid*., 3.

The notion of sovereignty over Russia's borders and in its "near-abroad," paranoia about "color revolutions," and a deep, consciously cultivated sense of historical insecurity all guide the Kremlin to use all means available to control the information space.[12] This effort includes cyber power.

China and Russia differ in how they conceptualize cyber and information operations and security in cyberspace. Russia's approach to domestic Internet control emphasizes traditional forms of offline coercion such as confusing and inconsistently enforced speech laws, security service harassment, and police brutality. Chinese efforts to control the Internet domestically put a greater emphasis on technical filtering and other digital forms of control.[13] China takes control of the domestic information space more seriously than Russia does; China's effort at control is well-organized and financed in comparison with Russia's efforts in the same area.[14]

While Moscow views cyber capabilities as a way to achieve information control, it also places a heavy emphasis on cyber operations as means of disruption for disruption's sake—as well as the value of cyber operations for supporting foreign and national security policy goals. Cyber operations can degrade an enemy's military communications, disrupt a foreign company's operations in Russia, and achieve other objectives by means that do not amount to a use of force. In comparison, the Chinese government does not currently use cyber operations in so disruptive and destructive a fashion.

Russia and China thus think differently about cyber operations and tactics. For example, Russian thinking about digital influence sits within the traditional Soviet frameworks like "reflexive control," which posits that an attacker can feed a target with specially prepared information and compel the target voluntarily to do what the attacker wants.[15] This approach to information operations draws on Marxist-Leninist precepts that assume everything in the world is scientifically understandable and governed by laws of behavior.[16]

It also draws on outright pseudoscientific conceptions of how to manipulate human behavior, such as the bogus field of "acmeology" promoted by such figures as senior GRU official

[12] Justin Sherman, *Russia's War for Control of Global Internet Governance* (Social Science Research Network, May 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119863, 5-7.

[13] Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: Public Affairs, 2015); Julien Nocetti, "Russia's 'dictatorship-of-the-law' approach to internet policy," *Internet Policy Review* (November 2015); Justin Sherman, *Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior* (Washington: Atlantic Council, July 2021).

[14] See Aitel, et al., fn. 3.

[15] For an excellent treatment of this concept, see Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* (2004): 237-256.

[16] Diane Chotikul, *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study* (Monterey: Naval Postgraduate School, July 1986), 13.

Aleksandr Starunskiy.[17] Chinese thinking appears to focus more on personal relationships and individuals and on remaking the international order in Beijing's favor rather than outright destruction.[18] Many Chinese scholars have felt the need to develop a Chinese-specific theory of information warfare. The resulting theories draw heavily on Chinese military art, theories, and doctrine.[19] Some Chinese information warfare terminology echoes that of Russian thinking, like "military deception," but many other terms go in a different direction than Russia's notions of reflexive control.[20]

Domestically, Russia has primarily relied on traditional political propaganda, control of mass media, and targeted repression, arrest, or assassination of identified political opponents to achieve social control, in contrast to China's more extensive technical interventions on the Internet and social media—and the extensive use of facial recognition and access to smartphones to supplement traditional, local party surveillance. Under the stress of the war in Ukraine, the Russian government has ramped up control over the Internet and social media providers as well as political repression based on surveillance of social media.[21]

[17] Gavin Wilde, "In Russia's Information War, a New Field of Study Gains Traction," *New Lines Magazine*, (September 14, 2022), https://newlinesmag.com/argument/in-russias-information-war-a-new-field-of-study-gains-traction/.

[18] Peter Mattis, "Contrasting China's and Russia's Influence Operations," *War on the Rocks* (January 16, 2018), https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations/. See also, Jean-Baptiste Jeangène Vilmer and Paul Charon, "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare," *War on the Rocks* (January 21, 2020), https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/; James Dobbins, Howard J. Shatz, and Ali Wyne, *Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue: Different Challenges, Different Responses* (Santa Monica: The RAND Corporation, 2019), https://www.rand.org/pubs/perspectives/PE310.html; Paul Stronski and Nicole Ng, *Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic* (Washington: Carnegie Endowment for International Peace, February 2018), https://carnegieendowment.org/2018/02/28/cooperation-and-competition-russia-and-china-in-central-asia-russian-far-east-and-arctic-pub-75673; Adam Segal, "Peering Into the Future of Sino-Russian Cyber Security Cooperation," *War on the Rocks*, (August 10, 2020), https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/.

[19] Timothy L. Thomas, *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice* (Fort Leavenworth: Foreign Military Studies Office, October 2000), 1.

[20] See, e.g., Timothy L. Thomas, *Russian and Chinese Information Warfare: Theory and Practice* (Fort Leavenworth: Foreign Military Studies Office, June 2004), 33.

[21] Paul Mozur, Adam Satariano, Aaron Krolik and Aliza Aufrichtig, "'They Are Watching': Inside Russia's Vast Surveillance State," *The New York Times*, (September 22, 2022).

Russian Doctrine

Publicly available Russian documents on military doctrine and policy "do not explicitly reference cyber operations."[22] Partly this fact reflects semantic and conceptual differences between Russian thinking and much western, especially U.S., thinking. Russian doctrine and thinking generally does not refer to "cyber" unless talking about western ideas. Instead, Russians use "information security," which encompasses technical elements like security and encryption, but also includes the flow of information, political stability, social norms, and regime security.

During the last two decades, references to "information security" and "information warfare" have become increasingly numerous. While Russian doctrine includes defense and offense involving information technologies and cyberspace, some analysts find that "officials' promulgations and military literature reveal a predilection for the development of offensive cyber capabilities and operations" rather than defensive operations.[23]

Russian documents, such as the 2000 *Information Security Doctrine*, define "information security" to cover everything from information flows to state security, whereas other official documents break "information warfare" into categories without an effort at a single, cohesive, rigid definition.[24]

This emphasis has evolved over the last two decades, and the history highlights how the Putin regime thinks about cyber and information warfare. Shortly after ascending to the presidency in December 1999, Putin signed Russia's *2000 Military Doctrine*, which replaced the previous military doctrine from 1993. While taking note of declines in the threat of large-scale war, the spread of local conflicts, and the intensification of regional arms races, it named "the exacerbation of information confrontation" as a main factor in the "military-political situation" of the day.[25] It stated that a main external threat was "hostile information (information-technical, information-

[22] Janne Hakala and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace* (Riga: NATO Strategic Communications Center of Excellence, June 2021), https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf, 5.

[23] Bilyana Lilly and Joe Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces* (Tallinn: NATO Cooperative Cyber Defense Center of Excellence, 2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf, 129. See also, Calder Walton, "What's Old is New Again: Cold War Lessons for Countering Disinformation," *Texas National Security Review* (Fall 2022).

[24] Blagovest Tashev, Michael Purcell, and Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU Journal* (Fall 2019), 129-147, https://www.usmcu.edu/Portals/218/CAOCL/files/RussiasInformationWarfare_MCUJ_Fall2019.pdf?ver=2019-11-19-093543-040, 132.

[25] *The Military Doctrine of the Russian Federation*. April 22, 2000. https://www.armscontrol.org/act/2000-05/russias-military-doctrine. See also, Katri Pynnöniemi and Martti J. Kari, *Russia's New Information Security Doctrine: Guarding a besieged cyber fortress* (Helsinki: Finnish Institute of International Affairs, December 2016).

psychological) operations that damage the military security of the Russian Federation and its allies."[26]

Russia distinguishes between information-technical warfare, targeted at technical systems, "which receive, collect, process, and transmit information" during war and armed conflict, and information-psychological warfare, targeted at foreign militaries and publics at all times.[27]

In the section on the main internal threats, the *2000 Military Doctrine* highlighted the danger of attacks on "facilities related to vital services or the information infrastructure."[28] Among its goals were improved "special information support for the Russian Federation Armed Forces and other troops and their command and control organs," "technical cover and restoration of means of communication," "information security," and ensuring "scientific, technical, technological, information, and resource independence in the development and production of the main types of military output."[29]

With regards to the nature of war, it declared that "A large-scale (regional) war may have an initial period, the main component of which is an intense armed struggle to gain the strategic initiative, preserve stable state and military command and control, achieve supremacy in the information sphere, and win (maintain) air superiority."[30] This discussion of information as a part of broader conflict and security is consistent with the assertion made in the *2000 Information Security Doctrine*, published later in the year, that "the national security of the Russian Federation substantially depends on the level of information security."[31]

The Russia-Georgia War in 2008 acted as a catalyst for the Russian Ministry of Defense to consider creating an official offensive and defensive cyber operations unit in order to correct "deficiencies" in the information space.[32] Not every Western distinction or concept is reflected in Russian doctrine and thinking or reflected in the same way. The more expansive concept of information security and interrelated ideas such as information operations and information warfare feed into how the current Russian government has inherited, cultivated, and maintained the Russian cyber ecosystem.

In 2010, Russia's new *Military Doctrine* stated that Russia would utilize "political, diplomatic, legal, economic, environmental, informational, military, and other instruments for the

---

[26] *Ibid.*

[27] Keir Giles and Anthony Seaboyer, "The Russian Information Warfare Construct," *Defense Research and Development Canada*, (October 2019), https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf, 9.

[28] *The Military Doctrine of the Russian Federation*. 2000., *op. cit.*

[29] *Ibid.*

[30] *Ibid.*

[31] *Information Security Doctrine of the Russian Federation*. 2000. 1.

[32] Connell and Vogler, *Russia's Approach to Cyber Warfare*, 8.

protection of the national interests of the Russian Federation and the interests of its allies."[33] It listed one of the main "internal military dangers" to Russia as "the disruption of the functioning of organs of state power, important state and military facilities, and the informational infrastructure of the Russian Federation."[34]

This new doctrine says that the characteristic features of contemporary military conflict are "the intensification of the role of information warfare"[35] and "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force."[36] Then, the doctrine listed numerous tasks for the Russian armed forces, including that they should "develop forces and resources for information warfare."[37]

In terms of the battlefield itself, the doctrine directs the Russian military to "improve the system of information support for the Armed Forces and other troops,"[38] "improve the quality of means of information exchange on the basis of the use of up-to-date technologies and international standards, as well as the single information field of the Armed Forces and other troops as part of the Russian Federation's information space,"[39] and "create basic information management systems and integrate them with the systems for command and control of weapons and the automation systems of command and control organs."[40]

The emphasis on information security and information conflict spanned the strategic, operational, and tactical levels of warfare—although one must remember that, in Russian official thinking, the concept of information warfare extends far beyond the battlefield. In the most recent Russian military operations in Ukraine, it therefore is surprising to see how little of this doctrine has actually been implemented. For example, Russian operations have exhibited almost a total failure to use secure communications and other, rudimentary information controls.[41]

Russia's *2014 Military Doctrine*'s references to information and conflict emphasized the Kremlin's growing concerns about information and the Internet, as well as a recognition that other states were increasingly developing their information and cyber capabilities and using them in conflict. The 2014 doctrine's general provisions stated that the Russian Federation is committed

[33] *The Military Doctrine of the Russian Federation*. February 5, 2010. https://carnegieendowment.org/files/2010russia_military_doctrine.pdf. 1.

[34] *Ibid.,* 4.

[35] *Ibid.,* 5.

[36] *Ibid.,* 6.

[37] *Ibid.,* 17.

[38] *Ibid*., 12.

[39] *Ibid*., 17.

[40] *Ibid.*

[41] Joe Sabala, "Intercepted Call Reveals Russian Frustration Over Defective Equipment," *The Defense Post* (June 20, 2022).

to "taking military measures for the protection of its national interests and the interests of its allies only after political, diplomatic, legal, economic, informational, and other non-violent instruments have been exhausted."[42]

Concerning military threats encountered by the Russian Federation, it stated that "there is a tendency towards shifting the military risks and military threats to the information space and the internal sphere of the Russian Federation."[43] It named several information-related risks:

- *External military risks* include the "use of information and communication technologies for the military-political purposes to take actions which run counter to international law, being aimed against sovereignty, political independence, territorial integrity of states, and posing threat to the international peace, security, global, and regional stability."[44] This statement might be considered amusing if not so obviously in conflict with Russia's invasion of Georgia in 2008, invasion of Ukraine in 2014, and second invasion of, and full-scale war against, Ukraine in 2022.
- *Internal military risks* include "activities aimed at changing by force the constitutional system of the Russian Federation; destabilizing domestic political and social situation in the country; disrupting the functioning of state administration bodies, important state and military facilities, and information infrastructure of the Russian Federation"; and "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."[45]

Current military conflicts, it said, have characteristics and features that include "exerting simultaneous pressure on the enemy throughout the enemy's territory in the global information space, airspace and outer space, and on land and sea."[46] It then said a task of the Russian armed forces is "to enhance capacity and means of information warfare."[47]

---

[42] *The Military Doctrine of the Russian Federation*. December 25, 2014. No. Pr.-2976. https://rusemb.org.uk/press/2029. See also, Polina Sinovets and Bettina Renz, *Russia's 2014 Military Doctrine and beyond: threat perceptions, capabilities and ambitions* (Rome: NATO Defense College, July 2015). On July 2, 2021, Russian President Vladimir Putin updated the national security guidelines for the first time in six years, approving the new version of the *National Security Strategy*. The new document calls for developing comprehensive partnership and strategic cooperation with China and a special strategic partnership with India. It says this policy aims to create mechanisms that ensure regional stability and security in the Asia-Pacific region.

[43] *Ibid.*

[44] *Ibid.*

[45] *Ibid.*

[46] *Ibid.*

[47] *Ibid.*

In 2022, the Russian government published a new policy concept focused on Russia's "humanitarian policy" abroad.[48] There is ongoing debate about the exact significance of the document, which serves as a complement to Russia's existing *Foreign Policy Doctrine*, but it still merits analysis. The centerpiece of the document is protecting Russian spiritual and moral values[49] and promoting and defending the idea of a "Russian world" (*Russkiy mir)*.[50]

It emphasizes the Russian idea of "sovereignty"—that is, regime control—over its own borders, saying that the peaceful coexistence of different populations in Russia over the centuries (and, absurdly, "tolerance" for dissent[51]) has led to an understanding that foreign actors imposing their values on Russia is unacceptable.[52] These are longstanding strains of thinking in Moscow. For example, Putin has referred to the idea of a "Russian world," related to Boris Yeltsin's 1992 idea of "compatriots abroad," to justify aggressive behavior in Russia's near abroad, including the illegal 2014 invasion and annexation of Crimea.[53]

The document stated that a central part of implementing Russia's humanitarian policy abroad is using technology to support Russia's information goals.[54] Developing Russian-language Internet platforms and services, it said, is increasingly important—and social media tools, including social networks, instant messengers, and blogs, are an effective tool of soft power.[55] It added that mass media broadly are powerful tools for influencing the consciousness of people and promoting specific information to those people.[56] Numerous other references to information influence in the document discuss aligning domestic and international portrayals of events,

---

[48] Russian Federation. Об утверждении Концепции гуманитарной политики Российской Федерации за рубежом (Concept of the Humanitarian Policy of the Russian Federation Abroad) (September 5, 2022). What follows are rough, paraphrased translations of the original text.

[49] *Ibid.*, Section 13(1).

[50] *Ibid.*, Section (9).

[51] Section 15(1) likewise asserts, incorrectly, that Russia is free from censorship restrictions.

[52] *Ibid.*, Section 7.

[53] Vladimir Putin, "On the Historical Unity of Russians and Ukrainians," *en.kremlin.ru*, July 12, 2021, http://en.kremlin.ru/events/president/news/66181; Vladimir Socor, "Putin Inflates 'Russian World' Identity, Claims Protection Rights," *Eurasia Daily Monitor* (July 2014); Moritz Pieper, "*Russkiy Mir:* The Geopolitics of Russian Compatriots Abroad," *Geopolitics* (2020): 756-779; Igor Zevelev, "The Russian World in Moscow's Strategy," (Washington: Center for Strategic & International Studies, August 22, 2016), https://www.csis.org/analysis/russian-world-moscows-strategy; Mikhail Suslov, "'Russian World' Concept: Post-Soviet Geopolitical Ideology and the Logic of 'Spheres of Influence,'" *Geopolitics* (2018): 330-353. See also, Maura Reynolds, "'Yes, He Would': Fiona Hill on Putin and Nukes," *Politico* (February 28, 2022), https://www.politico.com/news/magazine/2022/02/28/world-war-iii-already-there-00012340. In this regard, Putin is parroting Hitler. See Nicholas Rostow, "Consequences," *Naval War College Review*, (Autumn 2014): 41-45, 50-54, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1346&context=nwc-review

[54] *Ibid.*, Section 15(10).

[55] *Ibid.*, Section 26.

[56] *Ibid.*, Section 70.

bringing Russian narratives to as many foreign audiences as possible, spreading "objective" information about Russia, and promoting the idea of Russia as a digitally advanced country.[57]

Writing down ideas about cyber and information warfare is one thing—and operationalizing those ideas bureaucratically is another matter entirely. Just because these doctrines exist does not mean Russia has perfected the art and science of waging cyber and information warfare on the global stage. Russia, like every other country, faces numerous challenges in translating doctrinal thinking into effective tactical, operational, and strategic action. Nonetheless, Russia's information security, foreign policy, and military doctrines of the last two decades underscore a focus on employing nonmilitary means of warfare to undercut Russia's enemies.

In practice, the Russian government has carried out cyber operations before initiating armed military conflict to increase confusion, contribute to the "fog of war," and (in its view) assert control over the information environment. For example, in 2008, during the Russo-Georgian War, the Russian government used direct kinetic strikes against communications networks, such as Georgia's "main east-west fiber-optic line" (which Russia severed),[58] and seemingly encouraged Russian hackers to launch distributed denial-of-service (DDoS) attacks against Georgian websites.[59] In after action reviews, the Russian government identified flaws with its information activities in Georgia. Igor Panarin, the Dean of the Foreign Ministry's Academy for Future Diplomats, for example, declared that "the Caucasus demonstrated our utter inability to champion our goals and interests in the world information arena."[60]

Russian Use of Active Measures

The Russian use of information and the Internet has strong historical roots. For more than a century, the Russian state has used forgeries, disinformation laundered through front organizations, and other kinds of falsehood-propagation and propaganda as an important military and intelligence tool.[61] In the 1920s, for example, the Russian state covertly spread disinformation

---

[57] *Ibid.*, Sections 18, 19, 68, and 74.

[58] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgian War," *Security Dialogue* (February 2012): 3-24, https://www.jstor.org/stable/26301960, 8.

[59] John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times* (August 12, 2008), https://www.nytimes.com/2008/08/13/technology/13cyber.html; *Cyber Security and Politically, Socially, and Religiously Motivated Cyber Attacks*. Paul Cornish. Strasbourg: European Parliament, February 2009. https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf. 15.

[60] Timothy L. Thomas, "Russian Information Warfare Theory: The Consequences of August 2008," in Stephen J. Blank and Richard Weitz (eds), *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* (Carlisle: U.S. Army War College Press, 2010), 279.

[61] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), and Mark Galeotti, "Active Measures: Russia's Covert Global Reach," Chapter 14 in Graeme P. Herd, *Russia's Global Reach: A Security and Statecraft Assessment* (Garmisch-Partenkirchen: Marshall Center, 2021).

in western Europe to discredit émigré groups with the hopes of luring individuals back to Russia, where their fate was disagreeable at best.[62]

Mark Galeotti looks at "active measures" (*aktivnye meropriyatiya)* as covert and deniable political influence and subversion operations, from corruption and disinformation to assassination and sponsorship of coups.[63] The history of such Russian activities stretches to the Tsars. At least from the 1950s onward, Soviet "active measures" included the use of front organizations and the spread of false information.[64] Soviet active measures reflected the wartime thinking of the Soviet leadership.

During World War II, the British Special Operations Executive (SOE) and to a lesser extent the U.S. Office of Strategic Services (OSS) used similar tactics.[65] After the War, active measures increasingly became a central part of the KGB overseas mission.[66] Following World War II, the United States and United Kingdom disfavored active measures in part because of the risk of blow back—the appearance of the disinformation in the home country in addition to the country targeted.

Evolution of Russian Disinformation

The Internet and advances in information technology have brought profound changes in the technological context for active measures. Practices and goals have not changed so much as the technology. As they always have done, the Russians emphasize deniability, blur the lines between public diplomacy and propaganda, and use disinformation as a form political warfare.[67]

Russia kept some information operations structure in place following the USSR's demise. In the Soviet Union, the Army's Main Political Department (GLAVPUR), part of the Special

---

[62] Dennis Kux, "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters,* (1985), 1.

[63] Mark Galeotti, *Active Measures: Russia's Covert Geopolitical Operations* (Garmisch-Partenkirchen: European Center for Security Studies, June 2019), https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0.

[64] The Committee for State Security (KGB)'s Service A, which had as its primary mission running an active measures department, was originally Service D, meaning disinformation. Rid, *op. cit.*

[65] See Anthony Cave Brown, *Bodyguard of Lies* (New York: Harper & Row, 1975).

[66] This was made explicit by KGB Chairman Yuri Andropov in his Directive No. 0066 of 1982. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West* (London: Penguin Books, 2000), 316.

[67] Justin Sherman, "Digital Active Measures: Historical Roots of Contemporary Russian Cyber and Information Operations," *Georgetown Security Studies Review* (April 2022), 1-9, https://georgetownsecuritystudiesreview.org/wp-content/uploads/2022/04/92_Final-1.pdf. For more on U.S. efforts to combat this kind of Soviet activity during the Cold War, see Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,* (Washington: National Defense University Press, 2012), https://ndupress.ndu.edu/Media/News/News-Article-View/Article/717885/deception-disinformation-and-strategic-communications-how-one-interagency-group/.

Propaganda Directorate, ran psychological operations.[68] When the Soviet Union collapsed, the military transferred the propaganda directorate to the GRU (still often known by the initials used during the Soviet period) in an effort to preserve it and rebranded it in 1994 as GRU Unit 54777.[69] The unit still exists.[70]

This history underlies the Russian government's conception of cyber activity and the modern information space. And, of course, Putin was a member of the Soviet Union's KGB (later the FSB), with broad internal, external, intelligence, counterintelligence, and secret police functions. His own history is part of the continuity between the Soviet and present Russian systems of information activities.

Russian Cyber Operations in the Ukraine Conflict and Elsewhere

More recently, before the Putin regime's "special military operation" or large-scale war on Ukraine in 2022, the GRU launched DDoS attacks against Ukrainian banks and defense websites, and Russian hackers also placed wiper malware (malicious software designed to destroy or erase data) on Ukrainian computer systems.[71] At the outset of the 2022 invasion, Russia successfully engaged in cyber attacks against Ukraine's satellite communications systems and financial infrastructure.[72] These operations are consistent with Russia's tradition of using cyber as a means of conducting disruption, coercion, and sabotage operations without engaging in obviously impermissible coercion or armed conflict.

In Estonia in 2007, when the Estonian government decided to move a controversial, Soviet World War II memorial statue in the capital city Tallinn, hackers in Russia launched widespread DDoS attacks against major news outlets, banks, communications organizations, political parties,

[68] Andrei Soldatov and Michael Weiss, "Inside Russia's Secret Propaganda Unit," *New Lines Magazine*, (December 7, 2020), https://newlinesmag.com/reportage/inside-russias-secret-propaganda-unit/. See also, Ray C. Finch, "Ensuring the Political Loyalty of the Russian Soldier," *Military Review* (July-August 2020): 52-67, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2020/Finch-Russian-Political-Loyalty/.

[69] Soldatov and Weiss, "Inside Russia's Secret Propaganda Unit."

[70] See, e.g., Antonin Toianovski and Ellen Nakashima, "How Russia's military intelligence agency became the covert muscle in Putin's duels with the West," *The Washington Post*, (December 28, 2018), https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

[71] Kyle Fendorf and Jessie Miller, *Tracking Cyber Operations and Actors in the Russia-Ukraine War*, (New York: Council on Foreign Relations, March 24, 2022), https://www.cfr.org/blog/tracking-cyber-operatio ms-and-actors-russia-ukraine-war.

[72] Patrick Howell O'Neill, "Russia hacked an American satellite company one hour before the Ukraine invasion, *MIT Technology Review* (May 10, 2022). See also, Dan Goodin, "US and allies say Russia waged cyberattack took out satellite network, *Ars Technica* (May 10, 2022); James A. Lewis, *Cyber War and Ukraine* (Washington: Center for Strategic & International Studies, June 2022).

and the websites of the Estonian presidency and parliament.[73] In 2015 and 2016, following the Russian government's illegal invasion and annexation of Crimea and growing Russia-Ukraine tensions, the GRU hacked into and shut down power grids in Ukraine.[74]

In 2018, when the Organization for the Prohibition of Chemical Weapons (OPCW), whose stated mission is to implement the Chemical Weapons Convention, launched an investigation into the Russian government's poisoning of Sergei Skripal and his daughter, the Kremlin sent GRU agents to the Netherlands to hack into the OPCW and disrupt the investigation.[75] Substantial evidence exists that the Russian government uses cyber and information operations with greater frequency and openness in line with changes in Russian military doctrine and information strategy.

In foreign contexts, information warfare and information operations in Russia are "weapons as well as strategies that are deployed cumulatively over time, not just to disable an adversary's military machine, but also to demoralize and subvert it from within and isolate it from other networks abroad that could support it."[76] In 2017, the Defense Intelligence Agency (DIA) assessed that "Moscow views information and psychological warfare as a measure to neutralize adversary actions in peace to prevent escalation to crisis or war."[77] Russian practice has focused less on directing information capabilities against enemy forces in operations than against "the domestic 'nerves of government' or of society."[78]

Further, senior Russian officials have reiterated that "open conflict need not have been declared for hostile activity in information space to begin."[79] A Swedish Defense Research Agency analysis of Russian government documents on information warfare finds that the Russian conception is sweeping, not just in theory but in practice: "information warfare is not a service or

---

[73] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, (May 16, 2007), https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[74] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Andy Greenberg, "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction," *WIRED*, (September 12, 2019), https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

[75] https://www.opcw.org/about/mission. See, e.g., "How the Dutch foiled Russian 'cyber-attack' on OPCW," *BBC*, (October 4, 2018), https://www.bbc.com/news/world-europe-45747472.

[76] Stephen J. Blank, "Information Warfare a la Russe," in *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition*, eds. Phil Williams and Dighton Fiddner (Carlisle: U.S. Army War College Press, 2016), https://www.jstor.org/stable/pdf/resrep11980.11.pdf, 219. Cited in: Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington: Center for Naval Analyses, March 2017), https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf.

[77] *Russia Military Power: Building a Military to Support Great Power Aspirations*. DIA-11-1704-161. (Defense Intelligence Agency, 2017).

[78] *Ibid*., 219-220.

[79] Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, November 2016), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf, 10.

branch of its own, but includes elements from intelligence, deception on the operational level [*operativnaia maskirovka*], electronic warfare, communications, protected and automated command and control, information management among staffs, and also the defense of information systems from electronic warfare and computer network operations."[80]

[80] Ulrik Franke, *War by Non-Military Means: Understanding Russian Information Warfare,* (Stockholm: Swedish Defense Research Agency, March 2015). 14.

3. Russia's Cyber Ecosystem

The Russian government uses various actors to build cyber and information capabilities and launch cyber and information operations. Among other things, these actors support Moscow's cyber and information objectives, shaping other countries' decisions, expanding Russia's deterrent capabilities, and bolstering Russia's traditionally defined military power.[81]

While the government cultivates an ecosystem in which cybercrime and "patriotic hacking" thrives, it does not exercise total, constant control over every cyber and information actor in Russia. Instead, Moscow supports some actors regularly and others as needed. The cyber and information actors at Moscow's disposal include:

- Government cyber units, principally in the FSB, SVR, and GRU;
- Cybercriminals and individuals actively recruited by the government;
- "Entrepreneurial" hackers and developers to whom or which the government provides incentives to develop their own cyber and information capabilities and services for Russian intelligence community use;
- Hackers with mafia-style familial connections to the security services;
- Cyber and information front companies, set up and run by the government;
- Academic institutions and think tanks that help the government cultivate and recruit cyber and information talent and promote its "information security" vision;
- Patriotic hackers encouraged by the government; and
- Private military companies that offer, or could develop, cyber and information capabilities.

Of particular interest is the Russian government's "social contract" with cybercriminals and specific profiles of several significant Russian cyber actors, including cybersecurity companies Positive Technologies, Bi.Zone, and Angara Security. These firms provide important elements of Russia's offensive cyber capabilities and/or Russia's cyber talent ecosystem.

Government Cyber Units

On the state side, some of the most important Russian cyber units reside primarily within the Federal Security Service (FSB), the foreign intelligence service (SVR), and the military intelligence agency (GRU).

[81] *Annual Threat Assessment of the U.S. Intelligence Community*. (Office of the Director of National Intelligence, March 2022). https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Wstate-HainesA-20220308.pdf. 12.

FSB: The FSB is the successor to the Soviet Committee for State Security (KGB), the USSR's primary security agency. The Russian government website describes its mission in the broadest, national security terms.[82] It has largely a domestic focus, though like its predecessor, the FSB, it engages in some foreign operations, principally in Ukraine.[83] The FSB's Center 16 and Center 18 run cyber operations, including against foreign targets. Of particular note, the FSB recruits cybercriminals.

- *FSB Center 16:* The FSB Center for Radio-Electronic Intelligence by Means of Communication/aka Unit 71330/aka "Center 16" houses the FSB's signals intelligence (SIGINT) capabilities—including message interception, decryption, and processing—and has targeted healthcare, finance, energy, education, and government systems worldwide.[84] British intelligence has also tied FSB Center 16 to cyber operations targeting Russian dissidents, political opponents, and citizens.[85] In 2022, the Department of Justice charged multiple FSB Center 16 officers with hacking the industrial control systems in power generation facilities, to which access "would have provided the Russian government the ability to, among other things, disrupt and damage such computer systems at a future time of its choosing."[86]

---

[82] http://government.ru/en/department/113/.

[83] Until May 2022, the FSB's Fifth Service had remit over the Ukraine portfolio within the intelligence services. Irina Borogan and Andrei Soldatov, "The Shadow War: Putin Strips Spies of Ukraine Role," (Washington: Center for European Policy Analysis, May 9, 2022), https://cepa.org/the-shadow-war-putin-strips-spies-of-ukraine-role/. In a very recent Justice Department indictment, it was revealed that a Russian national worked to influence U.S. elections in coordination with the FSB, rather than the GRU or SVR. *United States v. Ionov* (22-cr-259)(USDC, MDFL, 2022). https://www.justice.gov/opa/press-release/file/1523096/download.

[84] Andrew S. Bowen, *Russian Cyber Units*.(Congressional Research Service, February 2022). https://crsreports.congress.gov/product/pdf/IF/IF11718.. See also United Kingdom Foreign, Commonwealth, & Development Office, "Russia's FSB malign activity: factsheet," *gov.uk*, (April 5, 2022), https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet; Department of Health and Human Services, *Major Cyber Organizations of the Russian Intelligence Services*. (, May 2022). https://www.hhs.gov/sites/default/files/major-cyber-orgs-of-russian-intelligence-services.pdf. The HHS slide cites from the talk given by Mandiant: Matthew McWhirt, Daniel Smith, Omar Toor, and Brian Turner, "Proactive Preparation and Hardening to Protect Against Destructive Attacks," *Mandiant.com*, January 14, 2022, https://www.mandiant.com/resources/protect-against-destructive-attacks.

[85] Of particular note are the September 2017 operation against an associate of opposition leader Alexei Navalny and a February 2020 attempt to hack into the systems of Putin critic Mikhail Khodorkovsky. See *Russia's FSB malign activity: factsheet," op. cit.*

[86] Department of Justice, "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide," *Justice.gov*, (March 24, 2022), https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical. See *United States v. Gladkikh*, (21-cr-442) (USDC, District of Columbia, 2021). This case focuses on the efforts of a Russian Ministry of Defense research institute to damage critical infrastructure outside the U.S. causing two separate emergency shutdowns at a foreign-targeted facility. This same group attempted to hack computers of a United States company

- *FSB Center 18:* The FSB Center for Information Security/aka Unit 64829/aka "Center 18" oversees domestic cyber operations and engages in some foreign cyber operations.[87] In 2019, a Russian court sentenced the Center's former deputy director, FSB Colonel Sergei Mikhailov, to 22 years in prison for allegedly passing classified information to Western authorities.[88]

SVR: The SVR, as Russia's foreign intelligence agency, is primarily interested in cyber espionage. Less is publicly known about the SVR's internal cyber structure than the FSB and GRU internal cyber structures.[89] The SVR has been identified as being behind campaigns against Western governments, including the cyber espionage campaign against SolarWinds.[90] The Federal Bureau of Investigation has observed the SVR moving away from planting malware on victim networks and towards targeting cloud systems to steal information.[91] The SVR has been linked to Cozy Bear, the Russian Advanced Persistent Threat actor. Cozy Bear may be part of the SVR or a nonstate group affiliated with or directed by the SVR. Here the relationship is obscure.[92]

GRU: The GRU is Russia's military intelligence agency, initially created by the Soviet Union in 1942.[93] Its worldwide operations include gathering intelligence and running clandestine operations in the physical world and the online space. Some of the most significant GRU units include:

---

responsible for managing critical infrastructure entities. A second indictment *United States v. Akulov, et al.*, (21-cr-20047)(USDC, District of Kansas, 2012) outlines a campaign by officers of Russia's Federal Security Service (FSB) to hack computers of hundreds of organizations connected to the energy sector worldwide. See also, Abraham Wagner and Nicholas Rostow, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2020) for an analysis of the various cases.

[87] Congressional Research Service. *Russian Cyber Units* (February 2, 2022). See also, Department of Health and Human Services. *Major Cyber Organizations of the Russian Intelligence Services* (May 19, 2022).

[88] Mike Eckel, "In Moscow Treason Trial, A Major Scandal For Russian Security Agency," *RadioFreeEurope/RadioLiberty*, (February 27, 2019), https://www.rferl.org/a/russia-hacker-mikhailov-stoyanov-fsb-scandal-for-russian-security-agency/29794092.html.

[89] Conversations had by Justin Sherman.

[90] *Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise*. (Cybersecurity & Infrastructure Security Agency, May 2021). https://www.cisa.gov/uscert/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf.

[91] "Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders," *CISA.gov*, (April 26, 2021), https://www.cisa.gov/uscert/ncas/alerts/aa21-116a.

[92] White House, "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," *WhiteHouse.gov*, (April 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[93] S.J., "What is the GRU?" *Economist*, (September 11, 2018), https://www.economist.com/the-economist-explains/2018/09/11/what-is-the-gru.

- *GRU Unit 26165:* The GRU 85th Main Special Service Center (GTsSS)/aka Unit 26165[94]/aka Fancy Bear/aka APT28 runs cyber and information operations in line with broader Russian military and political objectives. Among other things, it was behind the targeting of Russian performance art and anti-regime group Pussy Riot in 2015, spearphishing German political parties, and hacks of the World Anti-Doping Agency following its allegations of Russian doping at the Olympics and the Democratic National Committee in 2016.[95]
- *GRU Unit 74455:* The GRU Main Center for Special Technologies (GTsST)/aka Unit 74455[96]/aka Sandworm engages in more destructive attacks than Unit 26165. For example, it shut down power grids in Ukraine,[97] developed the NotPetya malware that spread globally and caused billions of dollars in economic damage,[98] and disrupted computer systems during the 2018 Olympics games.[99]
- *GRU Unit 54777:* The GRU 72nd Special Service Center/aka Unit 54777 is believed to run psychological (information) operations worldwide.[100] According to the Russian government, this information operations unit was formed in 2014 to protect Russian military control and communication systems and to prepare for cyber and information confrontation with a probable enemy.[101]

These security agencies' overall approaches to cyber operations are also reminiscent of their broader intelligence cultures and operational behavior. For example, the GRU is known to

---

[94] Department of Health and Human Services. *Major Cyber Organizations of the Russian Intelligence Services., op. cit.*

[95] *APT28: At the Center of the Storm* (Milpitas: FireEye, January 2017), https://www.mandiant.com/resources/report-apt28-a-window-into-russias-cyber-espionage-operations.

[96] Department of Health and Human Services. *Major Cyber Organizations of the Russian Intelligence Services., op. cit.*

[97] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, (March 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[98] Department of Justice, "Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," *Justice.gov*, (October 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and; Autumn Demberger, "Merck Awarded $1.4 Billion for NotPetya After 5 Years of Legal Battle," *Risk & Insurance*, (May 8, 2022), https://riskandinsurance.com/merck-awarded-1-4-billion-for-notpetya-after-5-years-of-legal-battle/; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[99] Andy Greenberg, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," *WIRED*, (October 17, 2019), https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

[100] Congressional Research Service. *Russian Cyber Units, op. cit.*

[101] « Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций », *TASS*, (March 12, 2014), https://tass.ru/politika/1179830.

carry out intelligence operations that employ physical violence. The GRU seems indifferent to whether or not its operatives become known.[102] GRU Unit 29155 operatives carry out assassinations, sabotage, and other more aggressive actions overseas and are routinely identified by intelligence agencies and investigative journalists. They continue notwithstanding public disclosure, perhaps believing that disclosure adds to their reputation and the fear generated by the GRU.[103]

Most famously, Unit 29155 operatives were allegedly responsible for poisoning former Russian spy Sergei Skripal and his daughter in 2018.[104] The unit has also been linked to poisonings in Bulgaria, Moscow's 2014 illegal annexation of Crimea, a failed coup in Montenegro, and the sabotage of a Czech ammunition depot, among other activities.[105] "Very little is off limits," MI6's then-chief said in 2019.[106]

In cyberspace, the GRU has shut down power grids in Ukraine,[107] launched the global *NotPetya* malware,[108] and routinely engages in other destructive and highly visible cyber operations. By contrast, the SVR, whose operations are premised on secrecy—including because

[102] There are complex factors at play and many theories around why this is the case, such as: the GRU uses outright sloppy tradecraft; it's not so much about not getting identified as it is not getting caught; its sloppiness is overblown; and the outright violence is meant as a signal to other dissidents and expats, among others. See, e.g.: Mark Galeotti, "GRU (GU) facing a little purge? If so, it's not spy less, but spy better," *In Moscow's Shadows*, (October 9, 2018), https://inmoscowsshadows.wordpress.com/2018/10/09/gru-gu-facing-a-little-purge-if-so-its-not-to-spy-less-but-spy-better/; Sebatian Roblin, "Why does Russia Turn to These Sloppy Assassins to Do the Dirty Work?" *The National Interest* (August 27, 2021), https://nationalinterest.org/blog/reboot/why-does-russia-turn-these-sloppy-assassins-do-dirty-work-192499; Andrew Roth, "String of own goals by Russian spies exposes a strange sloppiness," *The Guardian* (October 5, 2018), https://www.theguardian.com/world/2018/oct/05/string-of-own-goals-by-russian-gru-spies-reveals-new-trend-of-sloppiness.

[103] See, e.g., Mitch Prothero, "A secret Russian assassination squad has proved 'they can get to anyone' in Europe, but there's one problem. They're really sloppy," *Business Insider*, (October 9, 2019), https://www.businessinsider.com/gru-unit-29155-proves-they-can-get-to-anyone-but-theyre-really-sloppy-about-it-2019-10.

[104] "Factbox: Who are the Skripal poisoning suspects allegedly behind deadly Czech blast?" *Reuters*, (April 18, 2021), https://www.reuters.com/world/uk/who-are-skripal-poisoning-suspects-allegedly-behind-deadly-czech-blast-2021-04-18/.

[105] "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine," *Bellingcat*, (April 26, 2021), https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/.

[106] Sébastian Seibt, "Unit 29155, the Russian spies specializing in 'sabotage and assassinations,'" *France24*, (April 20, 2021), https://www.france24.com/en/europe/20210420-unit-29155-the-russian-spies-specialising-in-sabotage-and-assassinations.

[107] Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *op. cit.*

[108] Department of Justice, "Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware, " *op, cit.*

SVR operatives work undercover in embassies overseas—carries out covert cyber operations focused on espionage, like the SolarWinds hack.

Government Recruitment of Criminals and Individuals

Russian authorities recruit cybercriminals and individuals to develop cyber and information capabilities and run cyber and information operations on their behalf. Given its domestic security authority in Russia, the FSB recruits cybercriminals and other nonstate hackers and developers in Russia, in addition to other government security organs.

In 2017, for instance, the Department of Justice charged two FSB officers and two Russian nonstate hackers for stealing information from 500 million Yahoo accounts and then hacking emails from other services.[109] According to the indictment, the two FSB officers had "protected, directed, facilitated, and paid criminal hackers to collect information through computer intrusions in the U.S. and elsewhere."[110] One FSB officer was from Center 18, the FSB Center for Information Security.[111]

More recently, the Ukrainian security services identified five officers from the FSB's Crimea office as members of the Gamaredon hacking group as targeting the Ukrainian government on orders from the FSB's Center 18. This group has been active since 2013.[112] Notably, Gamaredon had a reputation for using off-the-shelf capabilities until developing its own custom malware in-house starting in 2017.[113]

The Russian government also recruits developers to run cyber operations and develop cyber capabilities, not just cybercriminals. In 2015, for example, Russia's defense conglomerate Rostec reportedly approached Alexander Vyarya, a developer at a Russian anti-DDoS software company, and asked him to attend a meeting in Bulgaria where he was asked to improve the government's DDoS attack capabilities.[114] During the session, the state software developers

[109] Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," *Justice.gov*, (March 15, 2017). Department of Health and Human Services. *Major Cyber Organizations of the Russian Intelligence Services*., *op. cit.*, See also *United States v. Dokuchaev* (17-cr-103)(USDC, NDCA, February 2017), https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

[110] *Ibid.*

[111] *Ibid.*

[112] Catalin Cimpanu, "Ukraine discloses identity of Gamaredon members, links it to Russia's FSB," *The Record*, (November 4, 2021), https://therecord.media/ukraine-discloses-identity-of-gamaredon-members-links-it-to-russias-fsb/.

[113] "Gamaredon Group," *Malpedia*, (accessed July 26, 2022), https://malpedia.caad.fkie.fraunhofer.de/actor/gamaredon_group; "The Top 5 Russian Cyber Threat Actors to Watch," *Rapid7.com*, (March 3, 2022), https://www.rapid7.com/blog/post/2022/03/03/the-top-5-russian-cyber-threat-actors-to-watch/.

[114] « Грузить по полной программе », *Meduza*, (September 3, 2015), https://meduza.io/feature/2015/09/03/gruzit-po-polnoy-programme.

showed Vyarya their existing DDoS capability. They demonstrated it against Ukrainian Ministry of Defense websites and the website for *Slon.ru*, a Russian online magazine. After this display of capabilities and intentions, Vyarya decided to flee Russia.[115]

"Entrepreneurial" Demonstration

Russian developers and hackers may also approach the Russian government with capabilities and service offerings, of their own volition, as part of the broader "adhocracy" set up by the Putin regime. It is a system "in which the president's favor is the main asset everyone wants to earn, and formal roles and responsibilities matter less than how one can be of use today."[116] This system leaves room for individuals, such as cybercriminals and talented programmers, to take the initiative.[117] After all, Putin is not a micromanager, and he creates incentives for individuals to be entrepreneurial.[118]

For example, when DDoS attacks hit an online Russian publication and Navalny supporters were targeted with phishing attacks in 2021, independent media outlet *Meduza* linked the DDoS attack to former FSB officer Pavel Seleznev.[119] According to *Meduza*, he had support from a Russian programmer, Mikahil Dudin.[120] *Meduza* learned that Dudin approached the FSB about a decade before with a "method for determining a user's specific location using cell towers," rather than sending cars with equipment to create a local network to track down a phone.[121]

Since then, Dudin reportedly has worked with the government to develop cyber capabilities and run cyber operations.[122] One source recently described his activities to *Meduza* as "all kinds of interesting projects" for Andrei Yarin,[123] the Chief of the Presidential Domestic Policy Directorate within the Russian Presidential Administration.[124] According to the Treasury Department, Yarin is responsible for countering Alexei Navalny's influence in Russian society,

---

[115] *Ibid.*

[116] Mark Galeotti, "Russia's Murderous Adhocracy," *The Moscow Times*, (August 22, 2020), https://www.themoscowtimes.com/2020/08/22/russias-murderous-adhocracy-a71219.

[117] *Ibid.*

[118] Fiona Hill and Clifford G. Gaddy, *What makes Putin tick, and what the West should do*, (Washington: Brookings Institution, January 13, 2017), https://www.brookings.edu/research/what-makes-putin-tick-and-what-the-west-should-do/.

[119] "'Your name is on some FSB officer's list,'" *Meduza*, (May 19, 2021), https://meduza.io/en/feature/2021/05/19/your-name-is-on-some-fsb-officer-s-list.

[120] *Ibid.*

[121] *Ibid.*

[122] *Ibid.*

[123] *Ibid.*

[124] President of Russia, "Presidential Executive Office subdivisions," *Kremlin.ru*, (last accessed August 1, 2022), http://en.kremlin.ru/structure/administration/departments.

"including through operations meant to discredit him."[125] This complex story highlighted the blurry area between state backing and state recruitment, when a developer voluntarily approached the Russian government and subsequently began working to run cyber operations against the Putin regime's enemies.

Mafia-Style Familial Entanglement

Some Russian cybercriminals have ties to the state that are more familial than business-like and contractual. These relationships echo a mafia-style model of nepotism and criminal networking. For example, the Russian hacking group "Evil Corp," which the United States indicted in November 2019 and sanctioned that December,[126] is run by Maxim Yakubets, a Russian hacker reportedly married to Alyona Eduardovna Benderskaya, the daughter of Eduard Bendersky.[127] Bendersky is a former FSB Spetsnaz officer, owner of multiple private Russian security firms, and what *Bellingcat* describes as a "de-facto spokesman for Department V,"[128] or Vympel, the FSB's externally focused "antiterrorist" unit[129] that has carried out multiple overseas assassinations.[130]

Since 2017, the year Yakubets appears to have married Bendersky's daughter, Yakubets has worked for the FSB, "to include acquiring confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf."[131] Since April 2018, Yakubets is outside U.S. jurisdiction and has been undergoing the process of getting a Russian government security clearance.[132]

---

[125] Department of the Treasury, "Treasury Sanctions Russian Officials in Response to the Novichok Poisoning of Aleksey Navalny," *Treasury.gov*, (March 2, 2021), https://home.treasury.gov/news/press-releases/jy0045.

[126] *United States v. Yakubets,* (19-cr-342)(USDC, WDPA, 2019), https://www.justice.gov/opa/press-release/file/1223586/download; Department of the Treasury, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware," *Treasury.gov*, (December 5, 2019), https://home.treasury.gov/news/press-releases/sm845.

[127] "The FSB's personal hackers," *Meduza*, (December 12, 2019), https://meduza.io/en/feature/2019/12/12/the-fsb-s-personal-hackers; Mark Krutov and Sergey Dobrynin, « Зять на 5 миллионов », *Svoboda*, (December 9, 2019), https://www.svoboda.org/a/30315952.html.

[128] "'V' for 'Vympel': FSB's Secretive Department 'V' Behind Assassination Of Georgian Asylum Seeker in Germany," *Bellingcat*, (February 17, 2020), https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/.

[129] Andrew S. Bowen, *Russian Military Intelligence: Background and Issues for Congress*, (Congressional Research Service, November 2021), https://sgp.fas.org/crs/intel/R46616.pdf.

[130] "'V' for 'Vympel'"; "FSB's Magnificent Seven: New Links between Berlin and Istanbul Assassinations," *Bellingcat*, (June 29, 2020), https://www.bellingcat.com/news/uk-and-europe/2020/06/29/fsbs-magnificent-seven-new-links-between-berlin-and-istanbul-assassinations/.

[131] Department of the Treasury, "Treasury Sanctions Evil Corp," *op. cit.*

[132] "The FSB's personal hackers"; *op. cit.*

Cyber and Information Front Companies

Russian security agencies set up front companies to disguise their cyber and information operations against foreign governments and populations. For example, in 2019, Czech magazine *Respekt* reported that the Czech Security Information Service (BIS), the country's domestic intelligence agency, had recently shut down a Russian intelligence operation that was using IT front companies to launch operations.[133] The intelligence operatives reportedly operated out of two computer equipment and software companies based in Prague, and their equipment was reportedly brought into the country in Russian diplomatic vehicles.[134]

Further, the Russian operatives were reportedly part of a larger international network.[135] This activity fits in line with Russian security agencies using front companies around the world for a variety of reasons, such as to evade sanctions and illicitly acquire Western military technology.[136] It also follows a pattern of Russian actors establishing front companies in the Czech Republic specifically: Putin aide and oligarch Yevgeny Prigozhin has established multiple Prague shell companies, as has at least one other individual in Russia laundering money.[137]

Establishing and using false front companies and false flag operations have a long history in Russia. For example, the Soviet Union set up numerous Communist front organizations during the Cold War to promote Soviet ideology, including in Cairo, Prague, Brussels, East Berlin, Budapest, Paris, and Helsinki.[138] The KGB also used organizations like state-run media outlet TASS and the Russian airline Aeroflot as cover for clandestine activities.[139]

---

[133] "Respekt: Czech intelligence uncovered Russian hackers using IT company front," *Radio Prague International*, (March 18, 2019), https://english.radio.cz/respekt-czech-intelligence-uncovered-russian-hackers-using-it-company-front-8135854.

[134] "Two Russian intelligence front companies uncovered in Czech Republic," *uawire.org*, (March 20, 2019), https://www.uawire.org/two-russian-intelligence-front-companies-uncovered-in-czech-republic.

[135] *Ibid.*

[136] See, e.g., Department of the Treasury, "Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," *Treasury.gov*, (March 31, 2022), https://home.treasury.gov/news/press-releases/jy0692; Sharon Weinberger, "Hacked Emails Reveal Russian Plans to Obtain Sensitive Western Tech," *The Intercept*, (May 28, 2015), https://theintercept.com/2015/05/28/u-s-cyber-firm-alleges-hacked-emails-reveal-russian-front-operation/; Department of Justice, "Russian National Receives 18 Month Prison Sentence for Smuggling High-Tech Night Vision Technology to Russia," *Justice.gov*, (October 9, 2014), https://www.justice.gov/nsd/pr/russian-national-receives-18-month-prison-sentence-smuggling-high-tech-night-vision.

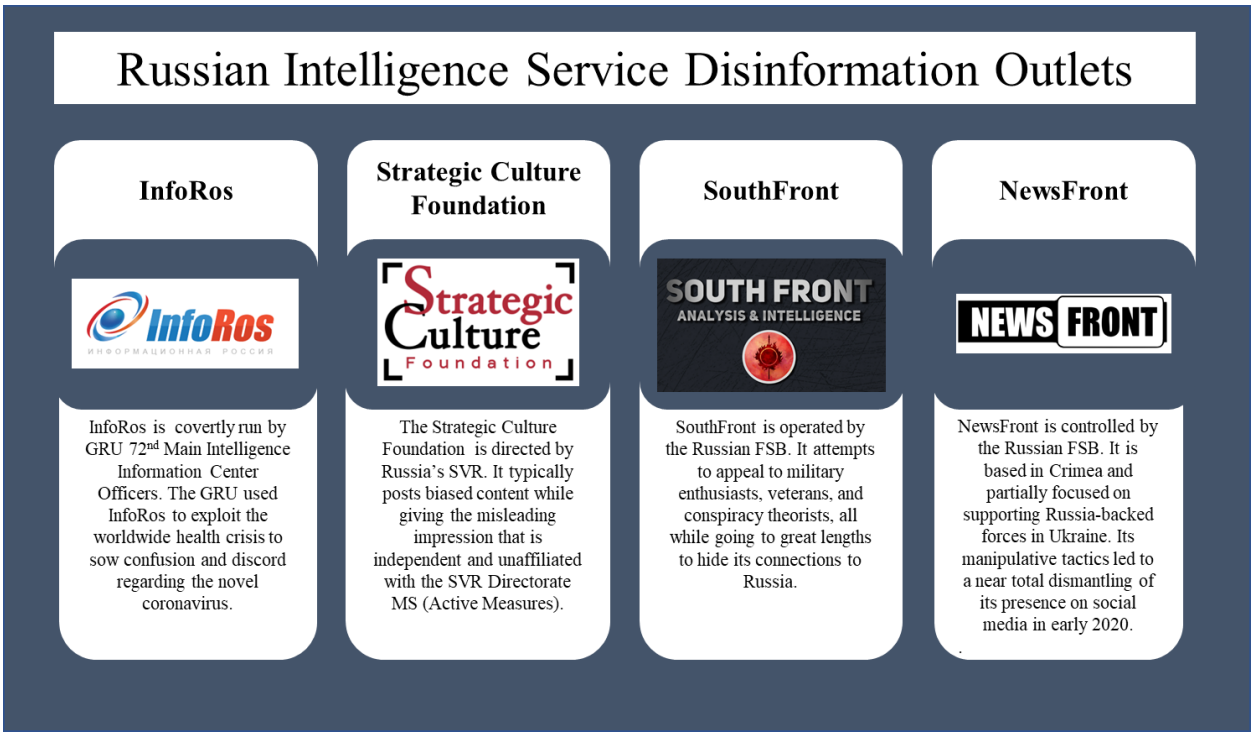
[137] Ivan Eckhardt, "Jurisdictional Risk: The Czech Republic," *DowJones.com*, (May 2020), https://www.dowjones.com/professional/risk/blog/czechrepublic/.

[138] *The Soviet Union and Nonruling Communist Parties*. SOV 82-10110X. (Central Intelligence Agency, August 1982. Declassified 1999). https://www.cia.gov/readingroom/docs/DOC_0000496805.pdf. 36.

[139] *Soviet and Chinese Communist Strategy and Tactics in North Africa, the Middle East, and South Asia*. *Special National Intelligence Estimate 10-2-65*. (Central Intelligence Agency, July 1965. Declassified August 1994). https://www.cia.gov/readingroom/docs/DOC_0000014188.pdf. 19.

In sanction decisions in April 2021, the Treasury Department exposed a number of such organizations: *InfoRos*, a collection of websites running disinformation for the GRU, the Strategic Culture Foundation, an online journal running disinformation for the SVR, *SouthFront*, a website running disinformation for the FSB, and *NewsFront*, a media outlet running disinformation for the FSB.[140] In particular, the GRU's 72nd Main Intelligence Information Center (GRITs), housed within Russia's "Information Operations Troops," which conducts cyber, information, and influence operations, runs InfoRos. One of its leaders, Denis Tyurin, was a former GRU officer.[141]

The SVR's Directorate MS, which runs "active measures," directs the Strategic Culture Foundation, which is also affiliated "closely" with Russia's Ministry of Foreign Affairs.[142] The FSB runs *SouthFront* and *NewsFront*, although, the Treasury Department describes *NewsFront* as "working with" FSB officers, perhaps suggesting informal oversight from the FSB compared to the oversight exercised over *SouthFront*.[143]



Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," (April 15, 2021)

[140] Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," *Treasury.gov*, (April 15, 2021), https://home.treasury.gov/news/press-releases/jy0126.

[141] *Ibid.*

[142] *Ibid.*

[143] *Ibid.*

While tasked by the Russian intelligence agencies, these information operations front groups did not necessarily receive funding, or receive all their funding, from the Russian government. Information subsequently released by the Treasury Department in March 2022 reveals that *SouthFront* solicited funding from its readers. Funding or lack thereof from the FSB was not specified.[144]

NewsFront was funded by Yuriy Sergeyevich Fedin, described by the UK government as an "entrepreneur" who used his company Intent to give money to *NewsFront*.[145] The Treasury Department also revealed that the SVR directs Oriental Review and New Eastern Outlook, two other disinformation outlets. Oriental Review is a website, and New Eastern Outlook is a "pseudo-academic publication" run by the Russian Academy of Science's Institute of Oriental Studies.[146] In addition to exposing more Russian disinformation front groups, the Treasury Department information highlighted the ways in which Russian academic institutions are entangled in this ecosystem as well.

Leveraging Academic Institutions and "Think Tanks"

Moscow leverages academic institutions and so-called think tanks to recruit cyber and information operations talent, develop such talent, and carry out activities in service of the Kremlin's political objectives.[147] For example, the Military Academy of Communications launched cybersecurity training in 2015.[148] The GRU has sponsored university "cadet classes" with computer and "patriotic education" lessons.[149]

The Information Security Institute (IISI), part of Moscow State University since 2003, works on commissioned projects for the Presidential Administration, including for the FSB and

[144] Department of the Treasury, "Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors," *Treasury.gov*, (March 3, 2022), https://home.treasury.gov/news/press-releases/jy0628.

[145] Her Majesty's Treasury. Office of Financial Sanctions Implementation. *Financial Sanctions Notice: Russia*, (London: Office of Financial Sanctions Implementation, April 2022). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1087942/Notice_Russia_040722.pdf. 4.

[146] Department of the Treasury, *Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors*, (March 3, 2022).

[147] The Russian government also recruits cyber talent from universities for other purposes, such as locating cybercriminals in Russia, though that is outside the scope of this paper. See, for example, "Moscow's cyber defense," *Meduza*, (July 19, 2017), https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense.

[148] Joe Cheravitch and Bilyana Lilly, *Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond* (Tallinn: NATO Cooperative Cyber Defense Center of Excellence, December 2020), https://ccdcoe.org/uploads/2020/12/2-Russias-Cyber-Limitations-in-Personnel-Recruitment-and-Innovation_ebook.pdf, 41.

[149] *Ibid.*

the Russian General Staff, which controls and houses the GRU.[150] Its director is a former KGB officer and a former deputy secretary of the Russian Security Council, and it appears to promote the Russian government's view of "information security" to the world, including by organizing an annual "information security" conference in Germany.[151]

According to the State Department, the Moscow think tank Katehon, a subsidiary of the pro-regime news company *Tsargrad*,[152] spreads disinformation and propaganda and has ties to the Russian intelligence community, such as through its advisory board, which it does not publicize on its website.[153] Each of these actors fits into the Kremlin's political influence and power projection strategy through use of the full range of information instruments: using diplomacy, spreading propaganda, running information operations, running cyber operations, financing domestic organizations, and leveraging regime sympathizers.[154] The Russian government does not necessarily need to fund these organizations or programs to leverage them to spread disinformation or cultivate cyber talent.[155]

Encouraging Patriotic Hackers

The Russian government encourages so-called patriotic hackers to run cyber and information operations, especially cyber operations, against foreign targets. The government knows that a media statement or televised speech can lead pro-regime hackers to act. In 2007, for example, unidentified cyber actors within Russia launched DDoS attacks against Estonian websites when the government decided to relocate a Soviet World War II monument in Tallinn.[156]

Most governments and observers believe that the Russian government encouraged the attacks to occur and most likely orchestrated them. Moscow expressed anger at the Estonian

[150] Carolina Vendil Pallin and Susanne Oxenstierna. *Russian Think Tanks and Soft Power*. (Stockholm: Swedish Defense Research Agency, August 2017).

[151] *Ibid.*, 38.

[152] See, e.g., Courtney Weaver, "God's TV, Russian style," *Financial Times*, (October 16, 2015), https://www.ft.com/content/27125702-71ec-11e5-ad6d-f4ed76f0900a.

[153] *Pillars of Russia's Disinformation and Propaganda Ecosystem*. (Department of State, August 2020). https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf. 56-57.

[154] See, for example, Geir Hågen Karlsen, "Divide and rule: Ten lessons about Russian political influence activities in Europe," *Palgrave Communications* (2019): https://www.nature.com/articles/s41599-019-0227-8.

[155] Anton Barbashin and Alexander Graefand, *Thinking Foreign Policy in Russia: Think Tanks and Grand Narratives* (Washington: Atlantic Council, November 2019), https://www.atlanticcouncil.org/in-depth-research-reports/report/thinking-foreign-policy-in-russia-think-tanks-and-grand-narratives/.

[156] Damien McGuinness, "How a cyber attack transformed Estonia," *BBC*, (April 27, 2017), https://www.bbc.com/news/39655415.

government: Putin said the decision "sows discord and mistrust."[157] Russian Foreign Minister Sergei Lavrov said, "this is blasphemous, and will have serious consequences for our relations with Estonia."[158] The Ministry added that Estonia's plan was "a blasphemous idea and a blatant mocking of the memories" of soldiers who fought in the Soviet Red Army.[159] A delegation of Russian parliamentarians, led by former FSB director Nikolai Koyalyov, went to Tallinn to "inspect" the memorial's relocation. When Kovalyov was in Tallinn, he called for the Estonian government to resign.[160]

The Russian Federation Council (upper house of parliament) released a statement calling on the government to take the "toughest possible measures against Estonia," describing the monument's relocation as "just one aspect of the policy, disastrous for Estonians, being conducted by provincial zealots of Nazism" interested in "the mockery of the remains of the fallen soldiers."[161] Following the DDoS attacks, a "commissar" in Nashi, the pro-Kremlin nationalist youth group, said he participated in the cyber operations against Estonia.[162]

Conceivably, the Russian government does not direct all such actions, but they appear to occur with Kremlin knowledge and encouragement. Such appears to be the case in 2022 when patriotic hackers targeted Ukraine.[163] Moscow does not hide its support for these groups and individuals. Putin himself stated in July 2017 that "hackers are free people. They are like artists. If they are in a good mood, they get up in the morning and begin painting their pictures."[164] He added, "Hackers are the same. They wake up in the morning, they read about some developments in international affairs, and if they have a patriotic mindset, then they try to make their own

---

[157] Francis Tapon, "The Bronze Soldier Explains Why Estonia Prepares For A Russian Cyberattack," *Forbes*, (July 7, 2018), https://www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/?sh=5455aca998c7.

[158] Steven Lee Myers, "Russia Rebukes Estonia for Moving Soviet Statue," *The New York Times*, (April 27, 2007), https://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html.

[159] David Mardiste, "Russia to Estonia: Don't move our statue," *Reuters*, (January 25, 2007), https://www.reuters.com/article/us-estonia-russia-statue/russia-to-estonia-dont-move-our-statue-idUSL2378719620070125.

[160] Victor Yasmann, "Russia: Monument Dispute With Estonia Gets Dirty," *Radio Free Europe/Radio Liberty*, (May 4, 2007), https://www.rferl.org/a/1076297.html.

[161] Pilvi Torsti, "Why do History Politics Matter?: The Case of the Estonian Bronze Soldier," *University of Helsinki*, (2008), https://helda.helsinki.fi/bitstream/handle/10224/4043/bronz_soldier2008.pdf?sequence=1, 29.

[162] Irina Borogan and Andrei Soldatov, "The Kremlin and the hackers: partners in crime?" *OpenDemocracy.net*, (April 25, 2012), https://www.opendemocracy.net/en/odr/kremlin-and-hackers-partners-in-crime/.

[163] See, e.g., Joe Tidy, "Russian vigilante hacker: 'I want to help beat Ukraine from my computer,'" *BBC*, (February 25, 2022), https://www.bbc.com/news/technology-60528594.

[164] "Putin Compares Hackers To 'Artists,' Says They Could Target Russia's Critics For 'Patriotic' Reasons," *Radio Free Europe/Radio Liberty*, (June 1, 2017), https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html.

contribution the way they consider right into the fight against those who have bad things to say about Russia."[165]

A substantial number of these actors believe in the Putin regime and their Russian "patriotism." As one American cybersecurity executive described this ecosystem in 2016, "most of those actors . . . are beholden and pay homage to the legacy and the power of the former Russian and Soviet regime. They do so by acting out patriotically."[166]

Private Military Companies

Russian private military companies (PMCs) are technically illegal in Russia. The Putin government nonetheless frequently employs them to project power.[167] While public information on Russian PMCs is limited,[168] there is at least one documented case of a Russian PMC focusing on cyber capabilities. The RSB Group (Russian Security Service Group) established a cyber detachment in 2016, which some reports describe, without further detail, as a "cyber defense" detachment.[169]

RSB Group primarily focuses on asset protection, training foreign entities, preventive electronic security measures, and other services.[170] Its establishment of a cyber unit is notable; that is almost all we know about it. Secrecy is a hallmark of Russian PMCs and their capabilities.

---

[165] *Ibid.*

[166] Matthew Dean and Catherine Herridge, "'Patriotic hackers' attacking on behalf of Mother Russia," *FOX News*, (January 16, 2016), https://www.foxnews.com/politics/patriotic-hackers-attacking-on-behalf-of-mother-russia.

[167] See, e.g., Seth G. Jones, et al., *Russia's Corporate Soldiers: The Global Expansion of Russia's Private Military Companies* (Washington: Center for Strategic & International Studies, July 2021), https://www.csis.org/analysis/russias-corporate-soldiers-global-expansion-russias-private-military-companies; Anna Borshchevskaya, *Russian Private Military Companies: Continuity and Evolution of the Model* (Philadelphia: Foreign Policy Research Institute, December 2019), https://www.fpri.org/article/2019/12/russian-private-military-companies-continuity-and-evolution-of-the-model/; Andrew S. Bowen. *Russian Private Military Companies (PMCs)*. (Congressional Research Service, September 2020). https://sgp.fas.org/crs/row/IF11650.pdf.

[168] For example, Sean McFate explains that "the industry is media-phobic, owing to its roots in the military, which traditionally eschews public scrutiny"; reporters are not usually allowed to interview "much less embed in" PMCs; and academics "depend almost entirely on the work of journalists for their analyses of these firms." Sean McFate, "Secrets of modern mercenaries: Inside the rise of private armies," *Salon*, (January 25, 2015), https://www.salon.com/2015/01/25/secrets_of_modern_mercenaries_inside_the_rise_of_private_armies/. See also, Sean McFate, *The Modern Mercenary: Private Armies and What They Mean for World Order* (Oxford: Oxford University Press, 2014).

[169] Margarete Klein, *Private military companies – a growing instrument in Russia's foreign and security policy toolbox* (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, June 2019), Hybrid CoE Strategic Analysis 17, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-17-2019.pdf, 2-3.

[170] Bristow, *Russia's Private Military Companies*, *op. cit.*, 2.

Much of the public knowledge about Russian PMCs and their weapons comes from journalist interviews with former Wagner Group fighters.

Alignment between Russian PMCs and other Russian cyber and information capabilities already exists. Most notable among them is the Wagner Group, because Yevgeny Prigozhin supervises both this Russian private military company and the state-backed Internet Research Agency (IRA) troll farm. It is possible that Russian PMCs may act in concert with other actors in the Russian cyber and information ecosystem, especially so when the same individual controls entities with these different sets of capabilities. Prigozhin's organizations appears to synchronize or coordinate efforts to project Russian state influence overseas. For instance, Prigozhin has reportedly deployed Wagner forces to the Central African Republic (CAR) while operating a company, Lobaye Invest, that finances CAR radio stations.[171]

Previously, in 2014, when Russian "little green men," including from the Wagner Group,[172] facilitated the Russian government's invasion and annexation of Crimea and the Donbas in Ukraine, other Prigozhin-owned entities, such as the Kharkov News Agency and organizations linked to the Internet Research Agency, promoted "pro-Russian, pro-separatist, and anti-Ukrainian propaganda and disinformation" simultaneously with the invasion.[173]

Russian PMCs are continually expanding their activities ("services") into areas such as human intelligence-gathering, drone reconnaissance, kidnapping, assassination, and information and cyber operations. Russian PMCs may use their Russian government encouraged capabilities to offer services on their own.

PMCs already approach foreign governments and offer essentially to "coup-proof" regimes. The ability to make good on such promises necessarily requires making assurances about repressing opposition. Russian PMCs may expand more into cyber capabilities if the Putin government becomes more dependent on these organizations to project power and/or encourages PMCs to become more proactive in developing capabilities they offer to clients overseas.

This expansion of activities could include developing capabilities in-house (e.g., by hiring Russian hackers) or acquiring capabilities off-the-shelf (e.g., from vendors that offer spyware on the commercial market). PMCs could also collaborate with the Russian government to acquire or develop cyber capabilities. For example, the FSB and GRU closely coordinate with some Russian PMCs in some areas of the world. Both agencies have in-house cyber capabilities, and they both have relationships with nonstate Russian hackers. While it is difficult to predict how the Russian

---

[171] Tim Lister, Sebastian Shukla, and Clarissa Ward, "Putin's Private Army," *CNN*, (August 2019), https://edition.cnn.com/interactive/2019/08/africa/putins-private-army-car-intl/.

[172] See, e.g., *Private Military Companies* (Geneva: United Nations Office of the High Commissioner for Human Rights, January 2015), https://www.ohchr.org/sites/default/files/Documents/issues/Mercenaries/WG/OtherStakeholders/ukrainian-hhru-submission-2.pdf; Illia Ponomarenko, "SBU says Russia's Wagner mercenaries involved in Donbas war," *Kyiv Post*, (October 7, 2017), https://www.kyivpost.com/ukraine-politics/sbu-readies-charge-russias-wagner-mercenaries-war-donbas.html.

[173] Jones et al., *Russia's Corporate Soldiers*, 27.

PMC and cyber landscape will change, greater PMC cyber involvement with the Russian state would be a foreseeable development.

The Kremlin's "Social Contract" with Cybercriminals

Cybercriminals operate in Russia in accordance with a generally understood "social contract" with the Kremlin. At its core, hackers must focus on targets outside of Russia, not undermine the Kremlin's objectives, and assist the state when asked. This applies for a range of hackers, whether organizations regularly tapped by the Russian security services or individuals with little contact with the Russian intelligence apparatus whatsoever.

The few, public examples of Russian government action against Russian nonstate hackers reflect this social contract. In March 2020, the FSB arrested 25 individuals, both Russian and foreign citizens, for running a digital identity theft ring which analysts suspected had Russians among its victims.[174] The Russian government's January 2022 claim that the FSB arrested members of the REvil ransomware group[175] is frequently cited as well, although it is highly likely these arrests merely constituted a Kremlin-orchestrated public relations stunt.

The Russian government may not approve of some security research activities, including those that expose or draw attention to the exposure of Russian citizens' information. In May 2021, Russian authorities arrested hacker Pavel Sitnikov, allegedly for posting the Anubis banking trojan's source code on his Telegram channel (Freedom F0x).[176] His wife, however, claims that the arrest was payback for Sitnikov's action in December 2020 exposing the Moscow Department of Health's leaking of over 300,000 Russians' health data online, a leak the government later called human error although it most likely resulted from poor system configurations.[177] Sitnikov sold malware as well.[178] Such sales seem less plausible as an explanation for his sudden arrest.

Company Profiles: From Small Vendors to Large Suppliers

Private-sector cybersecurity actors in Russia provide significant support to the Russian defense and intelligence community. Some of these companies also supply cybersecurity services to major Russian businesses. All of these companies play a central role in hiring top Russian cybersecurity talent apart from, and in addition to, those hired directly from educational institutions into government positions.

---

[174] Jeff Stone, "Rare cybercrime enforcement in Russia yields 25 arrests, shutters 'BuyBest' marketplace," *CyberScoop*, (March 25, 2020), https://www.cyberscoop.com/buybest-hackers-arrested-fsb-russia/.

[175] Carly Page, "Russia's FSB 'shuts down' notorious REvil ransomware gang," *TechCrunch*, (January 14, 2022), https://techcrunch.com/2022/01/14/fsb-revil-ransomware/.

[176] Catalin Cimpanu, "Russian hacker Pavel Sitnikov arrested for sharing malware source code," *The Record*, (May 31, 2021), https://therecord.media/russian-hacker-pavel-sitnikov-arrested-for-sharing-malware-source-code/.

[177] *Ibid.*

[178] *Ibid.*

Many of these companies are in difficult positions. While some actively and happily support the Russian defense and intelligence community, many Russian cybersecurity and technology companies for years did business with major Western organizations and have been forced to operate in an increasingly restrictive environment. They and their employees feel the effect of sanctions on Russia in response to the 2022 invasion of Ukraine and the Russian government's restrictions on private sector cybersecurity activity apart from what it needs.

Not every developer in Russia has the opportunity to leave the country, especially when they have family members, and their employment at Russian cybersecurity and technology companies does not necessarily equate to active support for the war on Ukraine or agreement with the Putin regime's behavior. The profiles below include Russian cybersecurity companies such as Angara Security, Bi.Zone, DeteAct, NTech Lab, Positive Technologies, Sberbank Technology, Security Code, Security Vision, Sovcombank Technologies, and Swordfish Security.

Profile: Angara Security

- Founded: 2015
- Online presence: Website | LinkedIn | Facebook | Instagram | Habr | TAdviser Profile (EN) | TAdviser Profile (RU)

Formerly Angara Technologies Group, Angara Security has been listed by TAdviser as one of Russia's 10 largest providers in the field of information security.[179] The company's revenue has "soared" over the last few fears—up 92% in 2021 from the year 2020 alone.[180]

Angara Security specializes in providing information security services for corporate businesses and government agencies.[181] It offers a range of services, from security analysis and penetration testing to regulatory compliance.[182] The Angara SOC Cyber Resilience Center (Angara SOC) offers monitoring and response services to help customers—primarily financial institutions—make informed decisions about information security processes.[183] The center uses

[179] « Angara Security, вошла топ-10 российских поставщиков ИБ-решений », *angarasecurity.ru*, (October 11, 2022), https://www.angarasecurity.ru/blog/angara-security-voshla-top-10-rossiyskikh-postavshchikov-ib-resheniy/; "Angara Security," *tadviser.com*, (accessed October 17, 2022), https://tadviser.com/index.php/Company:Angara_Security_(Angara_Technologies_Group,_AT_Group)_formerly_Angara_Technologies_Group.

[180] « Angara Security вошла топ-10 российских. »

[181] "Angara Technologies Group," *linkedin.com*, (accessed October 17, 2022), https://www.linkedin.com/company/компания-angara/.

[182] Angara Security, (accessed October 17, 2022), https://www.angarasecurity.ru.

[183] « Центр киберустойчивости Angara Soc, » *angaramss.ru*, (accessed October 17, 2022), https://www.angaramss.ru/soc/; « Тимур Зиннятуллин, Angara Security: Развитие коммерческого SOC — это дорога без конца », *cnews.ru*, (February 11, 2022), https://web.archive.org/web/20221013230923/https:/safe.cnews.ru/articles/2022-02-11_timur_zinnyatullin_angara_security.

the IRP/SOAR system made by Security Vision, considered below, to automate components of cybersecurity response procedures.[184]

Angara was founded by Sergey Sherstobitov (Сергей Шерстобитов, CEO) who previously worked for Informzashchita as General Director. In 2020, Sherstobitov pointed to the growing role of the state in information security, noting that there has been a trend of consolidation in IT assets, with many state-owned companies or companies with state participation acting as the largest buyers of these assets.[185] Sherstobitov stated he was wary of this trend, as he feared it would impede the quality and availability of services, and suggested that it may be necessary to adopt measures to limit government investment in IT infrastructure.

According to its website, Angara Security has partnered with other Russian cybersecurity companies, including Kaspersky, Positive Technologies, and Security Vision, and offers services to government agencies. Angara Security conducted a security assessment on behalf of the Committee on Informatization in the Kursk Oblast.[186]

Profile: BI.ZONE

- Founded: 2016
- Owned by Sberbank
- Online presence: Website (RU) | Website (EN) | Habr | Telegram | Telegram (Threat Zone) |Instagram | Medium | VK | Twitter | Facebook | LinkedIn | Github | TAdviser Profile (RU) | TAdviser Profile (EN) | CTFZone

Another one of TAdviser's largest information security providers in Russia, Bi.Zone was created in 2016 by Sberbank, Russia's largest financial institution.[187] Sberbank, which is subject to U.S. and EU sanctions, is in turn owned by Russia's Ministry of Finance (50% share) and domestic and international investors. Bi.Zone is a strategic digital risk management company that develops IT products for cybersecurity, implements security and risk assessments for its clients, and provides support services for security incidents. The enterprise provides services to a number

[184] "Angara Security: Implementation of Security Vision IRP/SOAR," *securityvision.ru*, (2021), https://www.securityvision.ru/en/projects/5163/.

[185] « Сергей Шерстобитов, Группа компаний Angara: Проблема ИБ вышла на уровень руководителей и собственников бизнеса » , *tadviser.ru*, (May 18, 2020), https://www.tadviser.ru/index.php/Статья:Сергей_Шерстобитов,_Группа_компаний_Angara:_Проблема_ИБ_вышла_на_уровень_руководителей_и_собственников_бизнеса.

[186] « Angara Security провела комплексную оценку ИБ в органах исполнительной власти Курской области », *angarasecurity.ru*, (accessed October 17, 2022), https://web.archive.org/web/20221014051846/https:/www.angarasecurity.ru/projects/gruppa-kompaniy-angara-provela-kompleksnuyu-otsenku-ib-v-organakh-ispolnitelnoy-vlasti-kurskoy-oblas/.

[187] « Обзор: Безопасность информационных систем », *tadviser.ru*, (October 3, 2022), https://www.tadviser.ru/index.php/Статья:Обзор:_Безопасность_информационных_систем; « Bi.zone », *tadviser.ru*, accessed October 17, 2022, https://web.archive.org/web/20221014050950/https://www.tadviser.ru/index.php/Статья:Обзор:_Безопасность_информационных_систем.

of global clients, such as Sber, KFC, and Bank St. Petersburg. In 2021, the company also opened a cybersecurity center in Qatar.[188]

Bi.Zone was a favored partner of a multitude of international organizations, acting as a strategic partner of INTERPOL, a cybersecurity adviser to the International Committee of the Red Cross (ICRC), and an expert organization of the Cyber Security Center at the World Economic Forum. It has also partnered with SWIFT, CREST, and the CyberPeace Institute.[189] Bi.Zone's Computer Emergency Response Team was a member of the FIRST (Forum of Incident Response and Security Teams) association but was suspended due to Russia's invasion of Ukraine.[190]

Bi.Zone is particularly well-known for being an enthusiastic sponsor of cybersecurity conferences and hacking competitions. Since 2018, it has organized an international conference on cybersecurity called OffZone where cybersecurity novices and experts alike attend educational workshops and participate in hacking activities. Several prominent Russian technology companies partner with Bi.Zone to organize the conference, including Positive Technologies, Angara Security, Sberbank, Kaspersky, Security Code, DeteAct, Swordfish Security, and Sovcombank Technologies.[191]

Bi.Zone hosts another international cybersecurity event known as Cyber Polygon that allows experts to come together for technical training and discussion.[192] The event is supported by both INTERPOL and the World Economic Forum, and prior speakers have included Steve Wozniak, the Prime Minister of Russia, the Executive Chairman of the World Economic Forum, and senior officials from INTERPOL, UNICEF, ICRC, IBM, Microsoft, Visa, Mastercard, Sber, and the nonprofit International Corporation for Assigned Names and Numbers (ICANN) that manages Internet domain names and IP addresses.[193]

In 2019, Bi.Zone's CEO, Dmitry Samartsev, claimed that Bi.Zone protected 80% of the Russian financial market "by collecting and analyzing large amounts of data about threats in [the] region," a metric with which no other cybersecurity company in the Russian market could

---

[188] "Bi.Zone," *tadviser.com*, (accessed October 17, 2022), https://tadviser.com/index.php/Company:BI.Zone.

[189] "Discover SWIFT," *swift.com*, (accessed October 17, 2022), https://www.swift.com/about-us/discover-swift/messaging-and-standards; "Trust and Assurance," CREST-approved.org, (accessed October 17, 2022), https://www.crest-approved.org; "CyberPeace Institute," cyberpeaceinstitute.org, (accessed October 17, 2022), https://cyberpeaceinstitute.org.

[190] "FIRST members around the world," *first.org*, (accessed October 17, 2022), https://www.first.org/members/map.

[191] "Sponsors and Partners," *offzone.moscow*, (accessed October 17, 2022), https://offzone.moscow/sponsors-and-partners/.

[192] "What is Cyber Polygon," *cyberpolygon.com*, (accessed October 17, 2022), https://cyberpolygon.com/about/; « Что такое Cyber Polygon », *cyberpolygon.com*, (accessed October 17, 2022), https://cyberpolygon.com/ru/about/.

[193] *Ibid*.

compete.[194] Although the company at the time sought to expand into Europe, current sanctions have halted the tech firm's advance.

Profile: DeteAct

- Founded: 2018
- Privately Funded
- Online presence: Website (EN) | Website (RU | LinkedIn | Twitter | Facebook | Blog (EN) | Blog (RU) | Github
- See also Decurity Twitter Facebook Github Linkedin

DeteAct was founded by Omar Ganeiv (Омар Ганиев), an application security and penetration testing expert who now teaches at MIREA, the Russian Technological University, one of the largest technical universities in Russia.[195] Although small, the company provides consulting services in several areas of cybersecurity: application security, penetration testing, security consulting, vulnerability management, DDoS testing, threat hunting, awareness training, bug bounty, blockchain security, and security research.[196]

DeteAct's website states that its employees are world hacking champions in capture the flag competitions and are among the "top 50 hackers in the world."[197] Clients are based in several regions, including the United States and EU, and are involved in industries such as payment and financial services, blockchain and crypto currency, artificial intelligence, email services, data brokering, and e-commerce. DeteAct has reportedly provided services for state corporations.

Although DeteAct had a large increase in revenue and employee growth in 2020, DeteAct's social media accounts have not been updated since October 2021.[198]

Profile: NTech Lab (Нтех Лаб)

- Founded: 2015
- Investors: Impulse VC, RT-Business Development, VB Partners, Mubadala, Russian Direct Investment Fund, Russian Foundation for Technological Development (Grant)

---

[194] World Economic Forum, "Dmitry Samartsev," *weforum.org*, (accessed October 17, 2022), https://www.weforum.org/people/dmitry-samartsev; "An inside look at Russia's cybersecurity market: a Q&A with BI.ZONE," *techradar.com*, (September 24, 2019), https://www.techradar.com/news/an-inside-look-at-russias-cybersecurity-market-a-qanda-with-bizone.

[195] « Хакинг как профессия: интервью с Омаром Ганиевым (Матфак'2012) », *math.hse.ru*, (December 20, 2021), https://math.hse.ru/news/544259495.html; "Omar Ganiev," 2018.offzone.moscow, (accessed October 18, 2022), https://2018.offzone.moscow/speakers/omar-ganiev/.

[196] "Introduction," *blog.deteact.com*, (April 22, 2018), https://blog.deteact.com/introduction/.

[197] "DeteAct Pentest," *deteact.ru*, (accessed October 18, 2022), https://deteact.ru.

[198] "DeteAct," *codeib.ru*, (December 14, 2020), https://web.archive.org/web/20221014062603/https:/codeib.ru/blog/itogi-koda-7/deteact-128?ysclid=l983nz7hwa144615465.

- Online Presence: Website (RU) | Website (EN) | Twitter | LinkedIn | Github | Youtube | VK | TAdviser Profile

NTech Lab conducts AI driven video analytics in face, silhouette, and vehicle recognition.[199] It is known for its analytics platform FindFace, a facial recognition system that has been used by individuals, companies, and governments.[200]

NTech Lab's founder, Artem Kukharenko, previously worked as a research scientist at Purdue University and as a software engineer for Samsung Research in Russia.[201] The company's co-founder Alexander Kabakov worked as a manager and producer at Newmedia Stars, a Russian internet company.[202] He created the Agency One digital communications agency in 2010, which serviced clients such as Russian Railways, Aeroflot, and Deutsche Bank, and became a managing partner of Typhoon Digital Development venture fund in 2013, among several other positions. Kabakov left NTech Lab's board of directors in December 2021 and Kukharenko departed the company's management shortly after, following the founders' loss of controlling shares of the company.[203]

The company has invested more than 1 billion rubles in developing its products and promoting them worldwide. In addition to its space in Latin America, NTech Lab recently opened an office in Thailand to facilitate growth in Southeast Asia.[204]

In 2021, the Department of Commerce National Institute of Standards and Technology (NIST) ranked NTechLab's facial recognition algorithm as the best in the world, although it appears to have been displaced since then.[205] In addition, the ODNI Intelligence Advanced

---

[199] "NTech Lab," *linkedin.com,* (accessed October 18, 2022), https://www.linkedin.com/company/ntechlab/.

[200] Shaun Walker, "Face recognition app taking Russia by storm may bring an end to public anonymity," *The Guardian*, (May 17, 2016), https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte.

[201] "Artem Kukharenko," *linkedin.com*, (accessed October 18, 2022), https://www.linkedin.com/in/aikuharenko/?originalSubdomain=ru; "Kukharenko Artyom Igorevich," *tadviser.com*, (accessed October 18, 2022), https://tadviser.com/index.php/Person:Kukharenko_Artem_Igorevich.

[202] "Kabakov Alexander Vladimirovich," *tadviser.ru*, (accessed October 19, 2022), https://tadviser.com/index.php/Person:Alexander_Vladimirovich_Kabakov.

[203] « Сооснователи NtechLab покинули компанию », *cnews.ru*, (July 6, 2022), https://www.cnews.ru/news/top/2022-07-06_soosnovateli_ntechlab_pokinuli?ysclid=l984kadek0591974293.

[204] "Award-winning facial recognition company NtechLab enters Thailand market," *Bangkok Post*, (August 26, 2022), https://www.bangkokpost.com/thailand/pr/2376965/award-winning-facial-recognition-company-ntechlab-enters-thailand-market.

[205] U.S. National Institute of Standards and Technology, "FRVT 1:1 Verification," *pages.nist.gov*, (accessed October 19, 2022), https://pages.nist.gov/frvt/html/frvt11.html.

Research Projects Activity (IARPA) awarded NTech Lab first place in two categories at the Face Recognition Prize Challenge in 2017.[206]

Ntech Lab has conducted projects for, among others, the Committee for Informatization and Communications of St. Petersburg, Indian Railways, the Ministry of Digital Development and Communications of the Novosibirsk Region, Moscow Oceanarium, the Department of Information Technologies of Moscow (DIT), the Department of Informatization of the Tyumen Region, the Main Directorate of the Ministry of Internal Affairs of Russia for St. Petersburg and the Leningrad Region, the Ministry of Internal Affairs of the Russian Federation (MVD), and the Ministry of Education of the Russian Federation.[207]

NTech Lab's facial recognition technology has been used in video surveillance systems in schools, universities, transportation systems, and residential buildings.[208] It was also deployed by Russian government officials to identify and issue warnings to individuals who violated quarantine requirements during Covid-19 outbreaks.[209]

NTech Lab made headlines in the summer of 2022, when Business Insider reported a leaked database revealing the names of over 1,100 entities from over 60 countries that had allegedly obtained a license to use FindFace, including Intel, SpaceX, Nokia, Philip Morris, Honeywell, Dell, Starlink, INTERPOL, the Royal Thai Army, the Russian Federal Security

[206] Stephen Mayhew, "NTechlab wins two categories at Face Recognition Prize Challenge," *biometricupdate.com*, (November 7, 2017), https://www.biometricupdate.com/201711/ntechlab-wins-two-categories-at-face-recognition-prize-challenge.

[207] « Нтех Лаб », *tadviser.ru*, (accessed October 19, 2022), https://www.tadviser.ru/index.php/Компания:NtechLab_(НтехЛаб)?ysclid=l984k56sm7906955597; Chris Burt, "India's RailTel plans facial recognition deployment at over 6K stations," *biometricupdate.com*, (July 12, 2022), https://www.biometricupdate.com/202207/indias-railtel-plans-facial-recognition-deployment-at-over-6k-stations.

[208] "In Moscow schools will launch a facial recognition system," *tadviser.com*, (accessed October 19, 2022), https://tadviser.com/index.php/Project:How_the_facial_recognition_system_is_arranged_in_Moscow; « Система распознавания лиц в Петербурге », *tadviser.ru*, (accessed October 19, 2022), https://www.tadviser.ru/index.php/Проект:Система_распознавания_лиц_в_Петербурге; Tyler Choi, "Sri Lankan university deploys NtechLab facial recognition for security, attendance," biometricupdate.com, (accessed May 27, 2022), https://www.biometricupdate.com/202205/sri-lankan-university-deploys-ntechlab-facial-recognition-for-security-attendance.

[209] "Biometric Solution Against Covid-19," *ntechlab.com*, (accessed October 19, 2022), https://ntechlab.com/solution/biometric-solution-against-covid-19/.

Service (FSB), and the Russian Federal Penitentiary system.[210] Both Nokia and Intel have denied using the technology.[211]

Profile: Positive Technologies (Позитив Текнолоджиз)

- Founded: 2002
- Online Presence: Website (RU) | Website (EN) | Habr | PTSecurity | Telegram | VK | Twitter | Github | TAdviser Profile (RU) | TAdviser Profile (EN)

One of Russia's largest information security companies, Positive Technologies provides computer network security solutions to clients such as Sberbank, Megafon, Mobile TeleSystems, Samsung, and the Russian Ministry of Defense.[212] The company has a reputation for excellent research and skilled employees, whose work "has earned the gratitude of such world names as Adobe, Apple, Google, Microsoft, Red Hat, and Siemens."[213]

Positive Technologies has formed technology partnerships with leading tech companies around the world, notably Microsoft, Kaspersky, and VMware.[214] The company opened offices in Sweden, Great Britain, the Czech Republic, Italy, India, Korea, Tunisia, the United Arab Emirates, and the United States.[215]

However, the U.S. government has long suspected that Positive Technologies engages in hacking operations, exploiting the vulnerabilities that it "discovers and publicizes."[216] The Treasury Department sanctioned Positive Technologies in 2021 for supporting Russian

[210] Caroline Haskins, "Intel, SpaceX, Philip Morris, and dozens of other US companies were in a leaked database of users for a Russian facial recognition company," *Business Insider*, (July 30, 2022), https://www.businessinsider.com/intel-spacex-philip-morris-leaked-database-users-ntech-russian-facial-recognition-company-2022-7.

[211] "Leaked List of NTech Lab Users Includes Intel, Dell, and Other US Companies," *findbiometrics.com*, (August 2, 2022), https://findbiometrics.com/leaked-list-of-ntech-lab-users-includes-intel-dell-and-other-us-companies/.

[212] « Российский рынок информационной безопасности по итогам 2021 года », tadviser.ru, (October 3, 2022), https://www.tadviser.ru/index.php/Статья:Обзор:_Безопасность_информационных_систем; *About Company* (Moscow: Positive Technologies, 2022), https://www.ptsecurity.com/upload/iblock/b44/e784q6nt0tmoj2ghzrfjnsc29bcok5u9/Company_History_2022.pdf.

[213] Patrick Howell O'Neill, "The $1 billion Russian cyber company that the US says hacks for Moscow," *MIT Technology Review*, (April 15, 2021), https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/; Positive Technologies, "Positive Technologies' key research activities in 2019-2021," *ptsecurity.com*, (April 20, 2021), https://www.ptsecurity.com/ww-en/analytics/positive-technologies-key-research-activities-in-2019-2021/.

[214] Positive Technologies, "Technology Partners," *ptsecurity.com*, (accessed October 19, 2022), https://www.ptsecurity.com/ww-en/partners/tech-partners/.

[215] *Ibid.*

[216] O'Neill, "The $1 billion Russian cyber company."

intelligence services and added the company to the Entity List for allegedly selling spyware to repressive governments.[217]

Along these lines, Positive Technologies organizes one of the largest cybersecurity conferences in Moscow, known as Positive Hack Days (PHDays) considered at greater length below. In many countries, these types of gatherings serve as fertile recruiting ground for intelligence operators, and PHDays appears to be no exception. Expert speakers deliver talks on cutting-edge issues in the field, participants discuss trends in the industry and attend workshops, and hackers compete in a variety of contests, showing off their skill.[218] Security Vision is a business partner for this event.

One of Positive Technologies' founders, Yury Maksimov (Юрий Владимирович Максимов), serves as the current head of the Board of Directors, after working as Technical Director and then CEO for several years. Maksimov started the company with his brother Dmitry and Evgeny Kireev.[219] He also acts as an advisor to the Minister for Digital Development, Communications, and Mass Media of the Russian Federation. As of August 2021, he was the majority shareholder in Positive Technologies.[220] Maksimov denies the U.S. government's accusations, claiming that Positive Technologies merely provides defense services to Russian government agencies.[221]

In December 2021, Positive Technologies became the first cybersecurity company to list on the Moscow Exchange.[222] In September 2022, the firm announced that it was launching a secondary public offering.[223]

---

[217] Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," *treasury.gov*, (April 15, 2021), https://home.treasury.gov/news/press-releases/jy0127; Department of Commerce, Bureau of Industry and Security. 15 CFR Part 744. RIN 0694-AI64. https://public-inspection.federalregister.gov/2021-24123.pdf.

[218] Patrick Reevell, "Inside one of the largest hacking conferences in Russia," *ABC News,* (May 17, 2018), https://abcnews.go.com/International/inside-largest-hacking-conferences-russia/story?id=55201815.

[219] Ирина Юзбекова, « Ловец хакеров: как программист Юрий Максимов построил компанию с миллиардной стоимостью и попал под санкции США », (April 15, 2021), https://www.forbes.ru/tehnologii/426487-lovec-hakerov-kak-programmist-yuriy-maksimov-bez-storonnih-investiciy-sozdal.

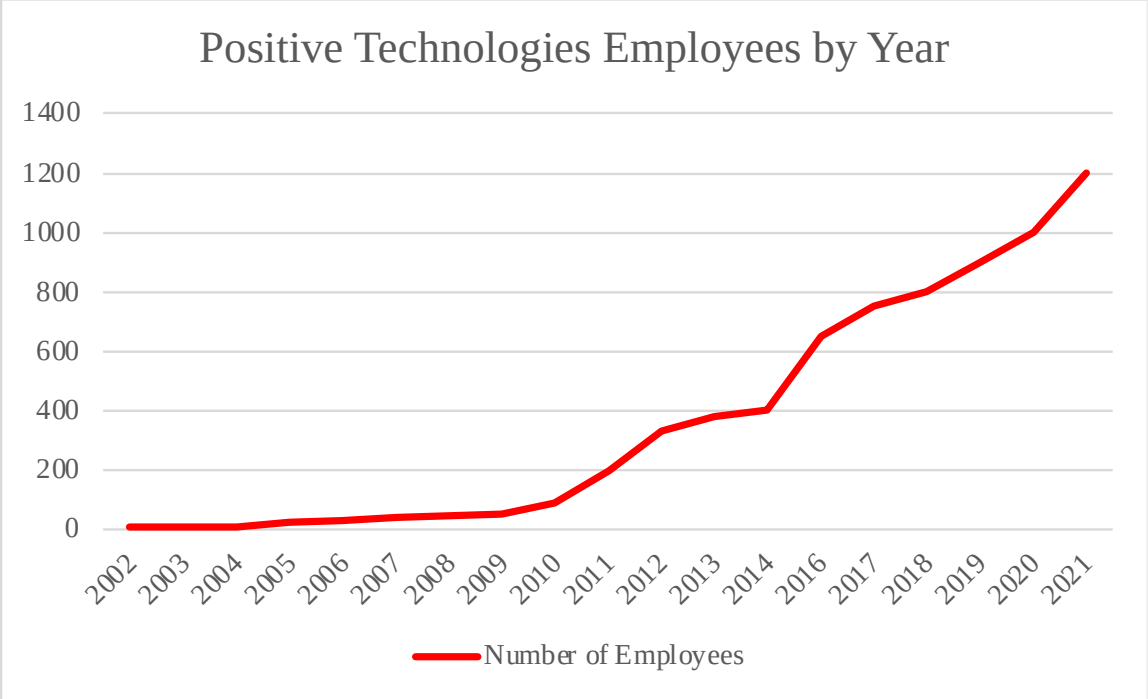
[220] Thomas Brewster, "This $500 Million Russian Cyber Mogul Planned To Take His Company Public—Then America Accused It Of Hacking For Putin's Spies," *Forbes,* (August 18, 2021), https://www.forbes.com/sites/thomasbrewster/2021/08/18/this-russian-cyber-mogul-planned-to-take-his-company-public-then-america-accused-it-of-hacking-for-putins-spies/?sh=79de1ef5cbe8.

[221] *Ibid*.

[222] Positive Technologies, "PJSC Positive Group lists on the Moscow Exchange and starts trading its shares," ptsecurity.com, (December 21, 2021), https://web.archive.org/web/20221014150806/https:/www.ptsecurity.com/ww-en/about/news/pjsc-positive-group-lists-on-the-moscow-exchange-and-starts-trading-its-shares/.

[223] "Russia's Positive Technologies launches secondary share offer," Reuters, (September 19, 2022), https://web.archive.org/web/20221014151020/https:/www.reuters.com/technology/russias-positive-

Positive Technologies has had significant growth over the past two decades—beginning with just 6 employees in a Moscow office in 2002, and now employing over 1,200 people.



Positive Technologies Employees by Year

Profile: Sberbank Technology

- Founded: 2011
- Owned by Sberbank
- Online Presence: Website | Habr (Career)

Like Bi.Zone, SberTech is an IT subsidiary of Sberbank. But in contrast to Bi.Zone, which serves customers around the world, SberTech's only client is Sberbank. The IT firm "operates in 16 regions of Russia" with approximately 11,000 employees and conducts over 500 IT projects a year for the Sberbank Group.[224] In addition, SberTech partners with the Skolkovo Innovation Center and coordinates with several universities to develop educational materials, train employees and students, and conduct research. At the Moscow Institute of Physics and Technology (MIPT),

technologies-launches-secondary-share-offering-2022-09-19/; Сергей Мингазов, « Positive Technologies объявила о начале вторичного размещения акций », *Forbes*, (September 19, 2022), https://www.forbes.ru/investicii/477425-positive-technologies-ob-avila-o-nacale-vtoricnogo-razmesenia-akcij.

[224] "Sberbank Technology," *sbergraduate.ru*, (accessed October 19, 2022), https://sbergraduate.ru/en/subdivisions/sberbank-technology/.

SberTech and MIPT have developed the Department of Banking Information Technologies, an educational program that offers bachelor's, master's, and postgraduate degrees of study.[225]

Sbertech's current CEO is Maxim Tyatyushev, who was appointed in June 2022.[226] He previously worked at NetCracker Technology before serving as managing director at Sberbank.

Sbertech's parent company, Sberbank, was removed from the global SWIFT messaging system in June 2022 as part of the European Union's sanctions against Russia in response to the invasion of Ukraine.[227] Moreover, the Deputy Chairman of the Board of Sberbank, Stanislav Kuznetsov (Станислав Кузнецов), has advocated prohibiting foreign operators and technologies from being used at critical infrastructure facilities.[228] Limiting access to domestic operators and encouraging a more active role of the state is particularly important for the cybersecurity of critical infrastructure because, according to Kuznetsov, "an organized cyber war is being waged against Russia."

A government commission meant to improve the sustainability of the Russian economy listed SberTech as a backbone organization, essential to the nation.

Profile: Security Code (Код Безопасности)

- Founded: 2008
- Owners: Philip Gens Georgievich (majority), Pyotr Valentinovich Efimov, Alla Vladimirovna Golova, Galina Bokova
- Online Presence: Website (RU) | Website (EN) | LinkedIn | Twitter | Facebook | Youtube | TAdviser Profile (RU) | TAdviser Profile (EN)

Security Code is a well-known cybersecurity firm in Russia. Its security products and services are implemented "by more than 32,000" organizations, and is listed by TAdviser as one of the Top 10 largest cybersecurity providers in the country.[229] It was once a subsidiary company

[225] « Кафедра банковских информационных технологий в МФТИ », *sbertech.ru*, (accessed October 19, 2022), https://sbertech.ru/mipt.

[226] "Tyatyushev Maxims Anatolyevich," *tadviser.com*, (accessed October 19, 2022), https://tadviser.com/index.php/Person:Maxim_Anatolyevich_Tyatyushev.

[227] "Sberbank Banned from SWIFT: Banking Sanctions Update for June 5 – 11, 2022," *rmahq.org*, (June 3, 2022), https://www.rmahq.org/blogs/2022/sberbank-banned-from-swift-banking-sanctions-update-for-june-5-11-2022/?gmssopc=1.

[228] « Безопасность критической информационной инфраструктуры РФ », *tadviser.ru*, (September 16, 2022), https://web.archive.org/web/20221014043709/https:/www.tadviser.ru/index.php/Статья:Безопасность_критической_информационной_инфраструктуры_РФ.

[229] "Security Code Ltd.," *linkedin.com*, (accessed October 19, 2022), https://www.linkedin.com/company/security-code-ltd./?originalSubdomain=ru.

of *Informzaschita*, before the majority ownership was transferred to Elena Bokova (81.5%), with the remaining shares divided between *Informzaschita*'s founders.[230]

Ownership then transferred in 2019 to Philip Gens, the son of the founder of the Lanit Group.[231] Lanit Group is a conglomerate composed of over 30 IT companies providing information technology services. Gens was appointed chairman of the board of directors for Lanit Group in 2017.

Security Code's current CEO, Andrei Golov (Андрей Голов), formerly worked as Deputy General Director at Energy Consulting and Deputy Commercial Director at Informzaschita.[232] He replaced the prior CEO, Anatoly Sharkov, in 2012.

Security Code's clients include the FSB, the Ministry of Defense, the Ministry of Internal Affairs, the Ministry of Justice, the Russian Prosecutor General, the Federal Security Guard Service, the National Guard (*Rosgvardia*), the Supreme Court, the Ministry of Finance, the Federal Treasury Department, the Federal Tax Inspectorate, the Central Bank, the Ministry of Health, and the Ministry of Foreign Affairs.[233] The company works with a wide range of state-owned and commercial companies, such as Sberbank, Liberty Insurance, and Western Union. It is also accredited as a testing laboratory of the FSB.

In 2018, Security Code and Kaspersky Lab entered into a partnership agreement that allowed Security Code to integrate a number of technologies from Kaspersky into its own products.[234]

Profile: Security Vision

Founded: 2007

Online Presence: Website (RU) | Website (EN) | LinkedIn (Security Intelligence)

Security Vision is a cybersecurity platform focused on automation in security governance, risk management and compliance, and security intelligence. The firm is listed in the Unified

[230] "About," *infosec.ru*, (accessed October 19, 2022), https://www.infosec.ru/about/; « Компании «Код Безопасности» (ГК «Информзащита») и «Альт Линукс» стали технологическими партнерами », securitycode.ru, (August 24, 2011), https://www-securitycode-ru.translate.goog/company/news/kompanii_kod_bezopasnosti_gk_informzashchita_i_alt_linuks_stali_tekhnologicheskimi_partnerami/?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp; « Код Безопасности », *tadviser.ru*, (accessed October 19, 2022), https://www.tadviser.ru/index.php/Компания:Код_Безопасности.

[231] "Gens Philip Georgievich," *tadviser.com*, (accessed October 19, 2022), https://tadviser.com/index.php/Person:Gens_Philipp_Georgievich.

[232] "Golov Andrey Viktorovich," *tadviser.com*, (accessed October 19, 2022), https://tadviser.com/index.php/Person:Golov_Andrei_Viktorovich.

[233] "Clients," *securitycode.net*, (accessed October 19, 2022), https://www.securitycode.net/clients/.

[234] « Бокова Елена Владимировна », *tadviser.ru*, (accessed October 19, 2022), https://www.tadviser.ru/index.php/Персона:Бокова_Елена_Владимировна.

Register of Russian Computer Programs and Databases of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation.[235]

Ruslan Rakhmetov serves as the company's CEO and formerly worked as the Director of the Information Security Competence Center of I.T. Co.[236] Among Security Vision's top managers is Ekaterina Cherun, who is responsible for sales and business development.[237] Cherun has previously worked at InfoWatch, Check Point, and Positive Technologies.

Security Intelligence LLC is a subsidiary brand of Security Vision that operates the company's research center within the Skolkovo Innovation Center.[238] It is located in Moscow's technology district and therefore benefits from close proximity and collaboration with peer enterprises and government supporters.[239]

Security Intelligence coordinates research projects with domestic universities to develop technologies that promote the automation of information security processes. Moreover, to help overcome the shortage of qualified IT specialists, Security Vision collaborates with schools, such as Moscow State Technical University, to give students opportunities with more practice-oriented educational models.[240]

Security Vision provides its IRP/SOAR system to major managed security service providers (MSSP), including Angara Security SOC.[241] It is also a sponsor of the computer security conference Positive Hack Days.[242] Kaspersky, Infowatch, HP, and IBM are listed among its technology partners.

---

[235] "Security Vision," *phdays.com*, (accessed October 19, 2022), https://www.phdays.com/en/about/sponsors/security-vision/.

[236] "Rakhmetov Ruslan," *tadviser.com*, (accessed October 19, 2022), https://tadviser.com/index.php/Person:Rakhmetov_Ruslan; *it.ru*, (accessed October 19, 2022), https://www.it.ru/gk_it/.

[237] "Ekaterina Cherun joined Security Vision management team," *securityvision.ru*, (March 2, 2021), https://www.securityvision.ru/en/news/ekaterina-cherun-joined-security-vision-management-team/.

[238] "Security Intelligence LLC," *securityvision.ru*, (accessed October 19, 2022), https://www.securityvision.ru/en/vendor/intellektualnaya-bezopasnost/.

[239] "Kremlin picks site for Russian 'Silicon Valley,'" *Reuters*, (March 18, 2010), https://www.reuters.com/article/idUSTRE62H33S20100318.

[240] Руслан Рахметов, « Security Vision: Российский бизнес заинтересован в предложениях от MSSP-провайдеров », *cnews.ru*, (September 7, 2022), https://web.archive.org/web/20221014105540/https:/safe.cnews.ru/articles/2022-09-07_ruslan_rahmetovsecurity_vision_rossijskij.

[241] Тимур Зиннятуллин, « Angara Security: Развитие коммерческого SOC — это дорога без конца », *cnews.ru*, (February 11, 2022), https://web.archive.org/web/20221014052728/https:/safe.cnews.ru/articles/2022-02-11_timur_zinnyatullin_angara_security.

[242] "Security Vision is a Positive Hack Days partner!" *securityvision.ru*, March 29, 2021, https://www.securityvision.ru/en/news/security-vision-is-a-positive-hack-days-partner/.

The company's clients include Sberbank, the FSB, the Pension Fund, Russian Post, the Bashkortostan Ministry of Labor and Social Protection, the Minister of Social Policy of the Krasnoyarsk region, the Sochi City Administration, the Federal Agency for Scientific Organizations, the Ministry of Sports, the Government of the Moscow Region, Moscow State University of Civil Engineering, Informzashchita, Jet Infosystems, and Rostec State Corporation. The Special Communications and Information Service of the FSB (Spetssvyaz FSO RF), the organ responsible for the organization and maintenance of special communications and information for government entities, adopted Security Vision's Security Operation Center in 2016.[243]

Profile: Sovcombank Technologies (Совкомбанк Технологии)

- Founded: 2021
- Owned by Sovcombank
- Online Presence: Website (RU) | Instagram | Habr | VK | TAdviser Profile

Sovcombank Technologies was formed by employees from the IT departments of Sovcombank Group, a major Russian financial institution, as well as invited external specialists. The subsidiary company provides IT services to all companies within Sovcombank Group. Employing approximately 2,000 IT personnel, Sovcombank Technologies conducts research investigating biometrics, artificial intelligence and its application in the financial sector, and other new technologies. The company is headed by Litovchenko Vyacheslav (Вячеслав Литовченко), who previously served as the deputy head of the IT department at Sovcombank.[244]

The United States and EU sanctioned Sovcombank and Sovcombank technologies after Russia's invasion of Ukraine.

Profile: Swordfish Security (Свордфиш Секьюрити)

- Founded: 2013
- Privately Funded
- Online Presence: Website (RU) | Website (EN) | Facebook | Twitter | Instagram | LinkedIn | Github | Habr | TAdviser Profile

Swordfish Security is a boutique security firm founded in St. Petersburg and also based in New York that focuses on consulting and IT services for clients in software development, finance, e-commerce, and professional services. Its clients include the Russian Post and Sberbank. According to the company's website, Swordfish Security has previously partnered with Positive Technologies.

[243] "Spetssvyaz FSO RF," *securityvision.ru,* (accessed October 19, 2022), https://www.securityvision.ru/en/projects/1906/.

[244] « Совкомбанк Технологии », *tadviser.ru,* (accessed October 19, 2022), https://web.archive.org/web/20221014091420/https:/www.tadviser.ru/index.php/Компания:Совкомбанк_Технологии.

Founder and CEO, Alex Pinaev, has extensive experience in management and business development.[245] He worked as an engineering manager at Motorola and Managing Director at Luxoft, staying with both jobs for several years before founding Swordfish Security in 2013. He has subsequently founded two other companies: Maverix, an application security correlation and orchestration platform, in 2017, which is currently based in Bellevue, Washington, and Mobix, a mobile application security testing tool, in 2022.[246]

Co-founder and Managing Partner, Yuri Sergeev, has a similarly impressive background.[247] Sergeev worked for several years at Luxoft (overlapping with Pinaev) as a Global Operations Manager and ISV Practice Director, with a short stint in between the two positions as the Head of Software Development Department at Asteros. Subsequently he served for a few years as the Head of Software Security Department at Sberbank Technology before founding Swordfish Security and Maverix with Pinaev.

Following Western sanctions on Russia due to the war in Ukraine, Swordfish Security has begun to focus on domestic production and domestic consumers, taking a "forced pause" in the international market.[248] The company will help facilitate clients switch to domestic software and IT services, following a presidential decree requiring critical infrastructure entities to move to Russian software by 2025.

---

[245] "Alex Pinaev," *linkedin.com*, (accessed October 19, 2022), https://www.linkedin.com/authwall?trk=gf&trkInfo=AQFwFroeaY8X6gAAAYPxzKBYgWqZtDd5OSMZvOk3MAD4EtfVvu9STa6SygJ6oYGpole8gRB_o_DQvovcY9isOcJPBpmps4yIVCj_6YobnatAcpEZ4MwDlhHnUTnF0LC2mP-ZEts=&original_referer=&sessionRedirect=https%3A%2F%2Fwww.linkedin.com%2Fin%2Fapinaev%2F.

[246] "Maverix," *linkedin.com*, (accessed October 19, 2022), https://www.linkedin.com/company/maverixco/; "Mobix," *linkedin.com*, (accessed October 19, 2022), https://www.linkedin.com/company/mobix-mobile/.

[247] "Yuri Sergeev," *linkedin.com*, (accessed October 19, 2022), https://www.linkedin.com/authwall?trk=bf&trkInfo=AQF2UmJ3QnxlZAAAAYPxzlnAOET0pyLsXIfE9Qg6pMfCcqs0aYg9JTsLYrTvNJcxNIfAIy6X5uOAgw35io6GEu48IQVnnU8NS78K-chg8PFoBMSENAkIKN-P8GPn6WgTg89q07M=&original_referer=&sessionRedirect=https%3A%2F%2Fwww.linkedin.com%2Fin%2Fyurisergeev%2Fdetails%2Fexperience%2F.

[248] « Цифровая безопасность хрупкого мира », *PBWM.ru*, (June 30, 2022), https://web.archive.org/web/20221014082650/https:/pbwm.ru/articles/tsifrovaya-bezopasnost-hrupkogo-mira.

4. Russia's Offensive Cyber Capabilities

The Russian government uses various instruments to build cyber capabilities and launch cyber and information operations, including by means of deception, misinformation, and disinformation. Russia also uses multiple approaches for building cyber capabilities and cultivating talent to expand its information ecosystem.

Precise estimates of Russian cyber and information forces are unknown, at least in the unclassified domain.[249] On an unclassified basis, CIA estimates that Russia, in addition to combat forces, has "approximately 100,000 other uniformed personnel performing command and control, cyber, support, logistics, and other functions in the military and security services."[250] A 2014 CIA estimate placed the number of collective FSB and SVR personnel at 400,000,[251] which would include everything from agents controlling human informants to those who conduct cyber operations.

The Russian government has developed a wide range of programs through which to train its cyber talent, especially emphasizing offensive capability development. Going forward, the acceleration of a Russian technology "brain drain" will be important.[252] This loss of skilled personnel will most likely weaken the Kremlin's near-term ability to maintain an up-to-date, innovative technology sector and a cyber talent pool.

[249] Good estimates most likely do not exist at any level of classification. U.S. intelligence estimates of the structure and personnel of Russian cyber and information units are a closely held secret. It is also hard to understand the structure of these organizations simply by observing operations, capability development, and other activities. For example, two Russian government cyber units may use similar techniques, but that is not necessarily a strong indicator of their degree of interconnection.

[250] Central Intelligence Agency, *Russia*, *CIA.gov*, (updated August 18, 2022), https://www.cia.gov/the-world-factbook/countries/russia/.

[251] Dakota Salavat Rice and Karl Bahm, *The Nature of Russian and Soviet Intelligence Agencies*, (Superior: University of Wisconsin, 2018), https://minds.wisconsin.edu/bitstream/handle/1793/79280/The%20Nature%20of%20Russian%20and%20Soviet%20Intelligence%20Agencies.pdf?sequence=9&isAllowed=y, 10.

[252] At the time of this writing hundreds of young Russians from the technology sector, including those trained in cyber, are fleeing Russia to avoid conscription into the military for the ongoing war in Ukraine. See, for example, Hundreds of Russia's top software developers may have left the country | New Scientist

Training the Russian Cyber Workforce

In September 2015, the Russian military academy launched a cybersecurity program to teach students cybersecurity concepts, robotics, network technology, and related topics.[253] Three months later, its first cadets began their service in the cyber field.[254] Cyber operations had already found their way into traditional Russian military coursework. The Soviet Union trained military personnel in psychological and information warfare, and Russia has continued to do so at the Military University of the Defense Ministry.

Following the Russo-Georgian War in 2009, the university integrated cyber activities like DDoS attacks into its information warfare curriculum.[255] Other military institutions, such as the Gagarin-Zhukovsky Combined Air Force Academy, teach students electronic warfare, information security, and information protection techniques.[256]

Non-military universities also teach cyber operations to students who will serve in the military. Voronezh State University gives courses on "information security" to students who will serve in officer positions in the Russian Armed Forces.[257] It offers topics such as information coding and compression algorithms, network security assessments, software vulnerability analysis, secure document management, and identifying people with biometrics.[258]

Students in the program work on projects with the Federal Service for Technical and Export Control, a Russian Ministry of Defense agency responsible for export licenses for weapons and dual-use technologies.[259] The agency is responsible for maintaining the "information security" of Russian military systems, foreign technical intelligence countermeasures in Russia, and protecting information generally.[260]

---

[253] Matthew Bodner, "Russian Military Launches Cybertraining Program for Youth," *The Moscow Times*, (September 1, 2015), https://www.themoscowtimes.com/2015/09/01/russian-military-launches-cybertraining-program-for-youth-a49276.

[254] « Российские вооруженные киберсилы », *Meduza*, (November 7, 2016), https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily.

[255] Bilyana Lilly and Joe Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, (May 2020) 143. The Past, Present, and Future of Russia's Cyber Strategy and Forces | IEEE Conference Publication | IEEE Xplore

[256] *Ucheba*, « Факультет радиоэлектронной борьбы и информационной безопасности ВУНЦ ВВС «ВВА» », *Voronezh.ucheba.ru*, (accessed September 16, 2022,) .

[257] Voronezh State University (Воронежский Государственный Университет), « Студентам военного учебного центра вручили дипломы по специальности «Компьютерная безопасность» », *mil.vsu.ru*, (February 18, 2022,) http://www.mil.vsu.ru/2022/02/18/студентам-военного-учебного-центра-в/.

[258] *Ibid*.

[259] *Ibid*.

[260] Russian Federal Service for Technical and Export Control, "Information on powers of FSTEC in Russia," *fstec.ru*, (accessed September 16, 2022), https://fstec.ru/en/359-powers.

In military exercises, Russian forces practice information operations such as dropping misleading leaflets and using loudspeakers for foreign-language broadcasts.[261] Military analysts have speculated that recent, substantial Russian military exercises like Vostok 2018 included testing large-scale *maskirovka* (military deception) ideas and tactics.[262] Russia may have intended the exercise to inform the West of the multi-dimensional, information and cyber capabilities of Russia's military force.[263]

An unclassified Intelligence Community briefing for the multinational Combined Joint Operations from the Sea Center of Excellence (CJOSCE) in May 2019 suggested that Russia's 2018 Vostok military exercise entailed the testing of *maskirovka* (concealment and deception) tactics, which include the use of agents provocateurs, information manipulation, and cyber operations.[264] Here *TV Zvezda*, run by the Russian Ministry of Defense, has already described this year's "Vostok-2022" military training exercise, held from September 1 to September 7, as an exercise in *maskirovka*.[265]

Russian intelligence organizations have their own training academies. These include the Military-Diplomatic Academy of the General Staff (for the GRU),[266] the FSB Academy (for the FSB), and the Academy of Foreign Intelligence (for the SVR).[267] Moscow protects the academies' secrecy. In 2018, for example, Russia arrested and imprisoned American Paul Whelan for

---

[261] Keir Giles, *Assessing Russia's Reorganized and Rearmed Military* (Washington: Carnegie Endowment for International Peace, May 2017), https://carnegieendowment.org/2017/05/03/assessing-russia-s-reorganized-and-rearmed-military-pub-69853, 9.

[262] Dave Johnson, "VOSTOK 2018: Ten years of Russian strategic exercises and warfare preparation," *NATO Review*, (December 20, 2018), https://www.nato.int/docu/review/articles/2018/12/20/vostok-2018-ten-years-of-russian-strategic-exercises-and-warfare-preparation/index.html.

[263] Mathieu Boulègue, "Russia's Vostok Exercises Were Both Serious Planning and a Show," *Chatham House*, (September 17, 2018), https://www.chathamhouse.org/2018/09/russias-vostok-exercises-were-both-serious-planning-and-show; Sergey Sukhankin, *Vostok-2018: An Alternative Analysis*, (Eesti, Estonia: International Center for Defense and Security, November 28, 2018), https://icds.ee/en/vostok-2018-an-alternative-analysis/; Vira Ratsiborynska, Daivis Petraitis, and Valeriy Akimenko, *Russia's Strategic Exercises: Messages and Implications* (Riga: NATO Strategic Communications Center of Excellence, July 2020), https://stratcomcoe.org/cuploads/pfiles/ru_strat_ex_29-07-e147a.pdf, 5-6.

[264] Office of the Director of National Intelligence. *МАСКИРОВКА: Russia's Masking of Its Real Intent*, (Briefing for the Combined Joint Operations from the Sea Center of Excellence, May 2015). http://www.cjoscoe.org/infosite/wp-content/uploads/2019/05/Maskirovka-Russias-Masking-of-its-Real-Intent.pdf. 3.

[265] « Маскировка, стрельба и проверка техники: в Бурятии провели подготовку к СКШУ «Восток-2022» », *TV Zvezda*, (August 30, 2022), .

[266] Andrew S. Bowen, *Russian Military Intelligence: Background and Issues for Congress*. (Washington: Congressional Research Service, November 2021). https://sgp.fas.org/crs/intel/R46616.pdf. 8.

[267] Gordon Bennett, *Russia's Foreign Intelligence Service*, (London: UK Conflict Studies Research Center, (March 2000), https://irp.fas.org/world/russia/svr/c103-gb.htm.

allegedly spying on an FSB-run university;[268] two years before, it reportedly punished dozens of new FSB agents for celebrating their graduation too publicly.[269]

At least one Russian government hacker, Aleksei Morenets, who belongs to a close-access hacking sub-team of GRU Unit 26165,[270] received training at the Alexander Mozhaysky Military Space Academy,[271] another GRU training facility, suggesting that perhaps other hackers are trained there as well. These academies have their own cyber-related training programs, but little information is publicly available about the security service training organizations.

The Russian military additionally uses its academic institutions to train cyber and information personnel in Kremlin-friendly countries. For example, the Krasnodar General S. Shtemenko Military Institute trains cadets to serve at the Russian military's Eighth Directorate, associated with "information defense," and it also trains information security-focused military personnel in the Collective Security Treaty Organization (CSTO), whose members include Russia, Belarus, Kazakhstan, Armenia, Kyrgyzstan, and Tajikistan.[272]

Moreover, the Russian security services recruit cyber talent from a wide swathe of Russian society, including universities, private-sector technical recruiting events, and criminal hacker forums. In 2013, Russian defense minister Sergei Shoigu said that he was on a "head hunt in the positive meaning of the word" for coders.[273] The Ministry of Defense subsequently bought advertising on the Russian social media platform VK to promote the "opportunity" and "comfortable accommodation" provided to individuals who join the Russian military's cyber forces.[274] The Russian IT firm Positive Technologies, which supports the Russian intelligence

---

[268] "Convicted US spy tried to gather information on students at FSB academy, says prosecutor," *TASS*, (November 8, 2021), https://tass.com/society/1358527; Jennifer Hansler, "Paul Whelan, an American detained in Russia, wonders why he was left behind," *CNN* (April 27, 2022), https://www.cnn.com/2022/04/27/politics/paul-whelan-left-behind-statement/index.html.

[269] Andrew Osborn, "Russian spy service punishes trainee agents for showy public celebration," *Reuters*, (July 14, 2016), https://www.reuters.com/article/us-russia-spies-scandal/russian-spy-service-punishes-trainee-agents-for-showy-public-celebration-idUSKCN0ZU26L.

[270] *United States vs. Morenets,* (18-cr-00263) (DC, WDPA, 2018). https://www.justice.gov/usao-wdpa/vw/us-v-Aleksei-Sergeyevich-Morenets. For an analysis of the Morenets case and related cases against Russian hackers see Abraham Wagner and Nicholas Rostow, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2020).

[271] "What is the GRU? Who gets recruited to be a spy? Why are they exposed so often?" *Meduza*, (November 6, 2018), https://meduza.io/en/feature/2018/11/06/what-is-the-gru-who-gets-recruited-to-be-a-spy-why-are-they-exposed-so-often.

[272] Volodymyr Lysenko and Catherine Brooks, "Russian information troops, disinformation, and democracy," *First Monday,* (May 2018), https://firstmonday.org/article/view/8176/7201.

[273] Andrew E. Kramer, "How Russia Recruited Elite Hackers for Its Cyberwar," *The New York Times*, (December 29, 2016), https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html.

[274] *Ibid*. Interestingly the "comfortable accommodation" displayed in one video was an apartment with a washing machine.

community's cyber capabilities, holds conferences that the FSB and the GRU use to recruit hackers.[275]

Russian authorities have a history of recruiting cyber talent from top Russian scientific universities. During the 1990s, Russia's Federal Agency of Government Communications and Information (FAPSI), a rough equivalent to the National Security Agency (NSA), responsible for signals intelligence and securing government information, recruited students from the Moscow Engineering Physics Institute, the Moscow Institute of Physics and Technology, and Moscow State University.[276]

By 2014, over 170 Russian universities were teaching their students about "information security."[277] For instance, St. Petersburg Electrotechnical University, one of Russia's oldest public universities, has an information security department whose graduates take jobs in law enforcement agencies, banks, telecommunication firms, and other businesses.[278]

The Russian government launched the ERA Technopolis (Технополис ЭРА) in 2018 to serve as a kind of quasi-military Silicon Valley and focus on developments in AI, robotics, information security, and computer science, among other areas.[279] ERA Technopolis aimed to accelerate the entry of young Russians into the defense- and military-technology complex.[280] Major defense and arms manufacturers, other private companies, and researchers co-locate there to develop next-generation technology and weaponry.[281]

According to the Treasury Department, ERA Technopolis has served as a home to military hackers and possibly fostered cyber and information capability development as well: it "houses and supports units of Russia's (GRU) responsible for offensive cyber and information operations and leverages the personnel and expertise of the Russian technology sector to develop military and dual-use technologies."[282] In April 2022, ERA Technopolis demonstrated some of its latest

[275] Department of the Treasury, *Treasury Sanctions Russia with Sweeping New Sanctions Authority*.

[276] Andrei Soldatov and Irina Borogan, *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities* (Washington: Center for European Policy Analysis, September 2022), https://cepa.org/russian-cyberwarfare-unpacking-the-kremlins-capabilities/, 9.

[277] *Ibid.*, 17.

[278] SPbSETU LETI (СПбГЭТУ ЛЭТИ), « Выпускники кафедры информационной безопасности », etu.ru, (accessed September 16, 2022), https://etu.ru/ru/fakultety/fkti/sostav/kafedra-cs/vypuskniki.

[279] Dominik P. Jankowski, *Russia and the Technological Race in an Era of Great Power Competition* (Washington: Center for Strategic & International Studies, September 2021), https://www.csis.org/analysis/russia-and-technological-race-era-great-power-competition, 3.

[280] Vladimir Sosnitsky, « ЭРА пополняется новобранцами из Тулы, » *Krasnaya Zvezda*, (August 5, 2019), http://redstar.ru/era-popolnyaetsya-novobrantsami-iz-tuly/.

[281] Katarzyna Zysk, "Defense innovation and the 4th industrial revolution in Russia," *Journal of Strategic Studies*, (2021): 543-571, 549-550.

[282] Department of the Treasury, *Treasury Sanctions Russia with Sweeping New Sanctions Authority*.

capability developments in cybersecurity, information, and artificial intelligence, among others, and said that the military already had tested most of the exhibits presented.[283]

Russian officials also use the prison system as a means of recruiting hackers, reportedly turning to criminal hackers and other IT professionals imprisoned in Russia to work for domestic businesses.[284] The same practice likely is used to support government cyber capability developments and even operations. The independent outlet *Meduza* reported in November 2016 that the Defense Ministry said years earlier it planned to call on "hackers who had problems with the law."[285]

The FSB and other security organs are publicly known to recruit criminal hackers who have not been charged with crimes. A substantial number of cybercriminals may enjoy a *krysha* (roof) of state protection, in line with how Russian state officials protect other criminals for a cut of the proceeds. It therefore would be logical if Russia recruited criminal hackers to its service.

While not the predominant focus of this paper, the Russian government's training of information operations personnel varies. There are uniformed personnel, such as those in the GRU's Information Troops, who receive "information security" and information operations training, probably in addition to standard GRU training. Russians conducting information operations outside the uniformed services may receive less extensive training than their uniformed counterparts. For example, the IRA troll farm hired untrained Russian citizens to work several-hour-length shifts posting content online.[286] The IRA would simply assign individuals particular keywords and subject lines to use in their articles and then instruct them to make posts based on that information.[287]

Balanced in Theory, Offensive in Practice

A recent review of Russian military documents and thinking around cyberspace concludes that "officials' promulgations and military literature reveal a predilection for the development of offensive cyber capabilities and operations, which are shaped by Russia's threat perceptions and doctrine, and the institutional cultures of the departments within the military conducting them."[288] Sergei Medvedev's study of Russian cyber capability finds that "although Russia has historically

---

[283] *Artificial Intelligence and Autonomy in Russia: Issue 39* (Arlington: Center for Naval Analyses, May 2022), https://www.cna.org/Newsletters/Ai%20and%20Autonomy%20in%20Russia/AI-and-autonomy-developments-in-Russia-Issue-39.pdf, 4-5.

[284] See, e.g., Brian Krebs, "Russia to Rent Tech-Savvy Prisoners to Corporate IT?" *Krebs On Security*, (May 2, 2022), https://krebsonsecurity.com/2022/05/russia-to-rent-tech-savvy-prisoners-to-corporate-it/.

[285] « Российские вооруженные киберсилы. »

[286] Adrian Chen, "The Agency," *The New York Times*, (June 2, 2015), https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[287] Neil MacFarquhar, "Inside the Russian Troll Factory: Zombies and a Breackneck Pace," *The New York Times*, (February 18, 2018), https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html.

[288] Lilly and Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, , *op. cit*, 129.

presented its posture as defensive, it is increasingly difficult to make that distinction."[289] Applying international relations theory about security dilemmas and offensive-defensive balances, Medvedev elaborates that "Russia's capabilities, perceptions, and posture in cyberspace, therefore, differ depending on one's perspective; it acts defensively relative to other great powers, but offensively as a would-be regional hegemon."[290]

Russian historical thinking, practice, and bureaucracy at a minimum shapes and informs Moscow's current approach to cyber capability development. The Soviet Union's offensive military orientation, as a declassified 1989 U.S. intelligence assessment put it, was "driven by the Soviet belief that only the strategic offensive offers the possibility of decisively defeating the opponent."[291]

Russian thinking emphasizes defense of the homeland and territorial integrity alongside "indirect action strategies and asymmetric responses across multiple domains to mitigate perceived imbalances."[292] Commentators have argued that the Russian government's "bunker mentality" is "deeply cultural" and rooted in centuries of concern about border insecurity and external threats and influences.[293] Some observers see this mentality at work today[294] and contributing to a predilection for offensive, rather than mostly defensive, cyber operations.

Insofar as intent is related to capabilities themselves, a substantial number of experts also have concluded that the Russian government is far more willing than the Chinese government to launch destructive cyber operations.[295] American cybersecurity official Rob Joyce has compared Moscow's cyber behavior to a hurricane and Beijing's to climate change—saying that if the Chinese government in cyberspace is "the long-term pacing threat," the Russian government in

---

[289] Sergei A. Medvedev. *Offense-Defense Theory Analysis of Russian Cyber Capability*. (Monterey: U.S. Naval Postgraduate School, March 2015), https://core.ac.uk/download/pdf/36737355.pdf. v.

[290] *Ibid*., 77.

[291] Central Intelligence Agency, *The Nature of Soviet Military Doctrine*, SOV 89-10037CX. (April 1989. Declassified April 2000). https://www.cia.gov/readingroom/docs/DOC_0000499601.pdf. 2. See also See https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-september-10 on Russia's information operations' shrinking area in the Ukraine War in recent days. How Russian forces performed during the ongoing Ukraine operation are a far cry from the decades old CIA study.

[292] Scott Boston and Dara Massicot, *The Russian Way of Warfare: A Primer*, (Santa Monica: The RAND Corporation, 2017), https://www.rand.org/pubs/perspectives/PE231.html, 2.

[293] See, e.g., Judy Dempsey, "Judy Asks: What Can the West Do About Russia's Bunker Mentality?" *Carnegie Europe*, (July 25, 2012), https://carnegieeurope.eu/strategiceurope/48939; Julia Gurganus and Eugene Rumer, *Russia's Global Ambitions in Global Perspective* (Washington: Carnegie Endowment for International Peace, February 2019), https://carnegieendowment.org/2019/02/20/russia-s-global-ambitions-in-perspective-pub-78067.

[294] Thomas Graham, "The Sources of Russia's Insecurity," *Survival*, (2010): 55-74.

[295] See, e.g., Joseph Marks, "Is Russia or China the biggest cyber threat? Experts are split," *The Washington Post*, (January 20, 2022), https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/.

cyberspace is louder and more destructive.[296] This preference for offensive action varies by Russian government organization. In cyberspace, the GRU is the most destructive, exploiting its relative operational autonomy to engage in aggressive, risky operations.[297]

The Office of the Director of National Intelligence's 2019 *Worldwide Threat Assessment* concluded that "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure" and that "Moscow is now staging cyber attack assets to allow it to disrupt or damage U.S. civilian and military infrastructure during a crisis."[298] Russia is not the sole actor in this area.

The U.S. Intelligence Community concluded that China "has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure" and presents a growing cyber attack threat. The 2019 *Worldwide Threat Assessment* further concluded that "China remains the most active strategic competitor responsible for cyber espionage against the U.S. Government, corporations, and allies."[299] Russia and China clearly create national security risks for the United States in cyberspace; although their approaches and actions differ, their overall goals appear similar.

In 2021, the *Worldwide Threat Assessment* stated that "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis." It concluded that Moscow "almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts."[300] The assessment once again noted that the Chinese government has cyber attack capabilities that threaten U.S. infrastructure, poses a growing attack threat in cyberspace, and "presents a prolific and effective cyber-espionage threat."[301]

---

[296] Peyton Doyle, "Rob Joyce: China represents biggest long-term cyberthreat," *Tech Target*, (June 9, 2022), https://www.techtarget.com/searchsecurity/news/252521338/Rob-Joyce-China-represents-biggest-long-term-cyberthreat. The Margin research team has recently concluded an extensive analysis of China's cyber operations. See Dave Aitel, et al, *Cyber Operations: The Rising Threat to American Security, op. cit.*

[297] Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services* (Berlin: European Council on Foreign Relations, May 2016), https://ecfr.eu/publication/putins_hydra_inside_russias_intelligence_services/, 2.

[298] Office of the Director of National Intelligence. *Worldwide Threat Assessment of the US Intelligence Community*. (January 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR-SSCI.pdf. 5-6.

[299] *Ibid*., 5.

[300] Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*. (April 2021). https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf. 10-11.

[301] *Ibid.*, 8.

The 2022 assessment followed in similar form, pointing out national security risks from both Beijing and Moscow, flagging that "Russia views cyber disruptions as a foreign policy lever."[302] This assessment stressed the persistence of disruptive and deceptive intentions.

The number of personnel dedicated to building enhanced offensive cyber capabilities supports this conclusion. While possibly anecdotal and not based on comprehensive data, a 2022 study by the International Institute for Strategic Studies (IISS) concluded that 33% of Russia's military cyber forces are focused on generating cyber effects.[303] According to the IISS estimate, this emphasis on producing cyber effects exceeds China's ambitions in this area (18.2%) and, of course, the U.S. interest (2.8%).[304]

It is important to recall that it is difficult to measure resource allocation with regard to creating cyber effects in the absence of reliable, public data on the subject. That said, it is well-known that Russia views "information warfare" as encompassing offense and defense, even if the term seems to imply a focus on offensive activity and capability development. Russian "information warfare" troops may be in charge of developing offensive mechanisms to run operations against Russia's enemies at the same time as they are building mechanisms designed to defend Russia from cyber attack.

Different Russian security agencies differ in their emphasis on destructive capabilities. All of the main Russian security organizations, the FSB, the GRU, and the SVR, focus on espionage and on developing offensive cyber capabilities that allow them to break into computer systems to steal information. The Russian military GRU, however, is uniquely focused on more destructive operations. In line with its overall tradecraft, it tends to engage in more noticeable, damaging cyber operations than counterparts like the SVR.[305]

---

[302] Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*. (February 2022), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf. 12.

[303] Mark Pomerleau, "Russia and China devote more cyber forces to offensive operations than US, says new report," *C4ISRNET*, (February 14, 2022), https://www.c4isrnet.com/cyber/2022/02/14/russia-and-china-devote-more-cyber-forces-to-offensive-operations-than-us-says-new-report/.

[304] *Ibid.*

[305] See, e.g., Mark Grzegorzewski and Christopher Marsh, *Incorporating the Cyberspace Domain: How Russia and China Exploit Asymmetric Advantages in Great Power Competition*, (West Point: Modern War Institute, March 15, 2021), https://mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/.

A Spectrum of Capabilities

The Russian government has demonstrated cyber capabilities that include phishing, DDoS attacks,[306] password brute-force algorithms,[307] ransomware,[308] and malware to shut down electrical grid Supervisory Control and Data Acquisition (SCADA) systems.[309] These capabilities have enabled the Russian security apparatus to break into systems abroad for surveillance purposes, ranging from hacks of the Georgian Ministry of Defense[310] to the widespread SolarWind espionage campaign against U.S. companies and businesses. They also give Russia the potential to inflict enormous damage on the U.S. and Western financial sector.

The Russian government has not shied away from using these capabilities. It has repeatedly disrupted Ukraine power grid operations and released the NotPetya malware that shut down global computer networks and cost the worldwide economy billions of dollars. In 2019, leaked documents reportedly from the Russian IT firm Sitek, a contractor for the FSB, detailed additional capability development such as technology to break the anonymity features of The Onion Router, popularly known as TOR.[311]

Moscow builds many of these capabilities in-house. For example, the 2018 Justice Department indictment of GRU officers for the hacking operation against the OPCW described GRU Unit 26165, an important military intelligence offensive cyber unit, developing its own malware in-house and managing its own command and control systems.[312] Other organizations investigating Russian government abuses and corruption have confirmed this finding.

The state also turns to programmers at companies and cybercriminals to develop capabilities. Russian hacker Mikhail Dudin volunteered his new surveillance capability and now

[306] Sergiu Gatlan, "White House pins Ukraine DDoS attacks on Russian GRU hackers," *Bleeping Computer*, (February 18, 2022), https://www.bleepingcomputer.com/news/security/white-house-pins-ukraine-ddos-attacks-on-russian-gru-hackers/.

[307] Department of Defense. *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*. PP-21-0782. (July 2021). https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF.

[308] "What is Petya and NotPetya Ransomware?" *Trellix*, (accessed September 6, 2022), https://www.trellix.com/en-us/security-awareness/ransomware/petya.html.

[309] Cybersecurity & Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure," *CISA.gov*, (February 25, 2016), https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

[310] Tom Fox-Brewster, "'State sponsored' Russian hacker group linked to cyber attacks on neighbors," *The Guardian*, (October 29, 2014), https://www.theguardian.com/technology/2014/oct/29/russian-hacker-group-cyber-attacks-apt28.

[311] Andrey Soshnikov and Svetlana Reuters, « Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ », *BBC Russia*, (July 19, 2019), https://www.bbc.com/russian/features-49050982.

[312] *United States vs. Morenets, et al*. (18-cr-263)(USDC, WDPA, October 2018), 10.

appears to work for the Presidential Administration, including to run cyber operations against regime opponents like Alexei Navalny.

Additionally, the Russian government on occasion may purchase cyber capabilities off-the-shelf. Emails published by WikiLeaks appeared to show the Italian surveillance company Hacking Team selling its Galileo Remote Control System (RCS) to the Kvant Scientific Research Institute,[313] a Russian research center put under FSB command more than a decade ago.[314] Specifically, Hacking Team appears to have sold its hacking software to Russian cybersecurity firm Advanced Monitoring, which then gave it to Kvant,[315] which is under the FSB's command and works on FSB-specific projects.[316] These kind of connections and operations may or may not be anomalies.

Case Study: State Recruitment from the Moscow Capture the Flag Competition

The Russian government has used capture the flag (CTF) competitions to recruit hackers. In 2010, Russia's Association of Chief Information Security Officers launched the annual Moscow Capture the Flag Competition with elite Russian university students, and the FSB began using the event to recruit hackers.[317] The Ministry of Defense followed suit in 2015 by starting to sponsor the event.[318] That year's top-ranking teams came from Bauman Moscow State Technical University, the Moscow Engineering Physics Institute, from which FAPSI recruited hackers, HSE University, the Russian military's Combined Arms Academy, and the National Research University of Electronics Technology.[319]

[313] Thomas Brewster, "Wikileaks Release: Hacking Team Says It Sold Spyware To FSB, Russia's Secret Police," *Forbes*, (July 9, 2015), https://www.forbes.com/sites/thomasbrewster/2015/07/09/wikileaks-hacking-team-fsb-sales/?sh=5f9e676455c7.

[314] Sergey Sukhankin, "Russia Beefs up Its Offensive Cyber Capabilities," *Eurasia Daily Monitor* (November 2016), https://jamestown.org/program/russia-beefs-offensive-cyber-capabilities/.

[315] Cyrus Farivar, "Hacking Team apparently violated EU rules in sale of spyware to Russian agency," *Ars Technica*, (July 17, 2015), https://arstechnica.com/tech-policy/2015/07/hacking-teams-surveillance-software-sold-to-kgb-successor/.

[316] Department of the Treasury, "Treasury Sanctions Russian Federal Security Service Enablers," *Treasury.gov*, (June 11, 2018), https://home.treasury.gov/news/press-releases/sm0410.

[317] Soldatov and Borogan, *Russian Cyberwarfare*, 17.

[318] *Ibid*.

[319] "Moscow Capture the Flag 2015," *mctf.aciso.ru*, (accessed September 15, 2022), http://mctf.aciso.ru/2015.html.

Russian university students at the 2018 Moscow Capture the Flag competition
The Moscow Technical University of Communications and Informatics was the host.[320]

Unlike state-affiliated CTF competitions in China, designed in part to signal Chinese cyber capabilities to the West,[321] there is little publicly available information about this competition. The 2020 webpage for the competition is no longer available. The 2021 webpage showed that day one of the event was devoted to workshops and lectures, and day two to the competitions.[322] Teams were composed of no more than seven university students, and competitions were in an attack/defense format.[323] That year's top teams came from similar universities as the 2015 competition, as well as a guest team, which was the only team without a university affiliation listed on the website.[324]

The 2021 Moscow Capture the Flag sponsors were the Russian telecommunications equipment supplier Voentelekom[325] and the Russian cybersecurity companies Security Code, Infotecs, and Kaspersky.[326] Infotecs is on the U.S. Commerce Department's Entities List for

[320] « «Код безопасности» наградил победителей финала соревнований Moscow Capture The Flag 2018 », *securitycore.ru*, (November 14, 2018), https://www.securitycode.ru/company/news/kod-bezopasnosti-nagradil-pobediteley-finala-sorevnovaniy-moscow-capture-the-flag-2018/.

[321] Dave Aitel, et. al, *China's Cyber Operations*, op. cit., 6; J.D. Work, "China Flaunts Its Offensive Cyber Power," *War on the Rocks*, (October 22, 2021), https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/.

[322] "Moscow Capture the Flag 2021," *mctf.aciso.ru*, (accessed September 15, 2022), http://mctf.aciso.ru.

[323] *Ibid*.

[324] *Ibid*.

[325] See more on the former CEO's long career in technology in the Russian government: "Yakunin Alexander Sergeyevich," *tadviser.com*, (accessed September 15, 2022), https://tadviser.com/index.php/Person:Yakunin_Alexander_Sergeyevich.

[326] "Moscow Capture the Flag 2021."

enabling "the activities of malicious Russian cyber actors."[327] It also works with the FSB and many other Russian government organizations and has links to a Russian businessperson allegedly supporting Russian influence operations.[328]

By scraping all the code posted for competitions from 2018-2021, and then unpacking the relevant information, it was then possible to analyze it. The results show competitors working on projects ranging from secure search engine development to penetration testing computer systems. At least one Russian hacker who helped assemble the code for the competition in 2018 formerly worked at Positive Technologies, the U.S.-sanctioned Russian IT company supporting the Russian intelligence community.

The 2018 projects are broken into "quals" and "final," ostensibly referring to qualifier rounds and a final round, respectively. The qualifier coding challenges were described as "reverse-forensic-medium," "crypto-easy-02," "stegano-easy," "forensic-medium," "reverse-hard," "recon-medium," "web hard," "pwn-medium," "web-medium," "reverse-medium-02," "reverse-medium-01," "reverse-easy," "web-easy-02," "web-easy-01," "crypto-easy-01," and "crypto-hard." The final round coding challenges were described as "abob_cloud," "boards," "Tactics1994," and "Shebetun."[329]

For example, one of the people uploading code for the competition, Egor Bogomolov, is based in Moscow and currently runs a company by the name of Singleton Security. The company is a Russian LLC registered in Moscow and appears, based on Google Maps imagery, to be located at a residential address.

[327] "Addition of Certain Entities to the Entity List, Revision of an Entry on the Entity List and Removal of an Entity From the Entity List," Rule by the Industry and Security Bureau, *Federal Register*, 83 FR 48532, (September 26, 2018), https://www.federalregister.gov/documents/2018/09/26/2018-20954/addition-of-certain-entities-to-the-entity-list-revision-of-an-entry-on-the-entity-list-and-removal.

[328] Scott Stedman, "Russian Cybersecurity Firm Draws U.S. Federal Scrutiny, Concern from National Security Experts," *Forensic News*, (January 20, 2022), https://forensicnews.net/russian-cybersecurity-firm-infotecs-draws-u-s-federal-scrutiny-concern-from-national-security-experts/; « Лицензии », infotecs.ru, (accessed September 15, 2022), https://infotecs.ru/about/license/.

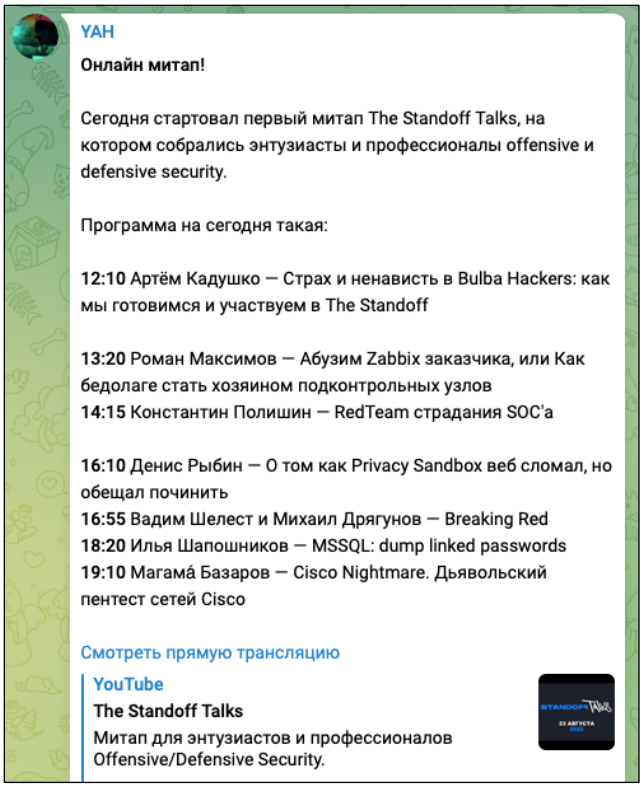
[329] One individual who uploaded code for the 2018 competition did so from the email address *e.bogomolov@Windows10.local*. Another email uploading code for the 2018 competition did so from the address *empty.jack@protonmail.com*. Both the first name initial ("e") and the last name ("bogomolov"), as well as the email name "empty.jack," match an individual by the name of Egor Bogomolov. Self-described as a "security specialist" and "application security specialist," Bogomolov, on his LinkedIn profile, lists his Telegram as @empty_jack and his primary email address as empty.jack@yandex.ru. Both these handles mirror the email addresses used to upload the CTF competition code. His LinkedIn also lists one of his specialties as "development and creation of tasks for CTF tournaments."

Bogomolov is active on Telegram[330] and speaks at universities about cybersecurity issues, such as the Russian Technology University (abbreviated MIREA).[331] He lists his current skills as web application security analysis (BlackBox, GreyBox, WhiteBox,), mobile application security analysis (iOS, Android), network technologies, Windows/Linux security, docker infrastructure (docker / docker-compos), code analysis (PHP, Python, Java, C#), developing software products to automate security analysis tasks, preparing reports on improving information security, conducting security analyses through social engineering, and conducting research in the cybersecurity field. He also lists one of his achievements as entry into the Yandex Bug Bounty Hall of Fame, though the link to the Yandex webpage is dead.

Previously, Bogomolov ran information security for the company HackerU and was a self-employed cybersecurity expert (Apr. 2020-Oct. 2021) and was a penetration tester at Wallarm in Moscow (Feb. 2019-Jan. 2020), Bi.ZONE (March 2018 - February 2019), and InfoSec (Информзащита) (December 2016 - March 2018). From October 2015 to December 2016, he worked as a signature analyst at Positive Technologies, the company that supports Russian intelligence community cyber operations. He also hosts online "meetups" with fellow Russian hackers.

[330] Telegram, @empty_jack, https://t.me/YAH_Channel.

[331] MIREA Student Union, post on *VKontakte*, (December 10, 2021), https://m.vk.com/wall-1236_19171.



Another frequent competition code contributor in 2018 uses the email address *mail@kitsu.me*. Per that address' website, the email belongs to Eugene Minibaev, a Russian software engineer interested in low-level programming (e.g., networking, hardware interaction) and programming languages. The Research Gate profile for Eugene Minibaev currently lists him as a master's student at Moscow State University's Department of System Programming, but the currency of that information is unclear.[332] The only other paper listed on Minibaev's profile is titled "Domain-specific debugger for QEMU dynamic binary translation system."[333]

One of the 2021 contributors, from the email address *sshkurov@matterport.com*, appears to be Sergey Shkurov, a Berlin-based Russian software engineer. He worked on projects for the virtual tour platform Matterport from May 2021 to June 2022, in Moscow, and now he works at the online German broker Trade Republic in Berlin—indicating he also left Russia in the past couple months. He studied at Moscow Technical University of Communications and Informatics and graduated with a bachelor's degree in Informatics in 2021.

Case Study: State Involvement with Skolkovo's CTF Russian Cup

Another prominent CTF held in Russia is the CTF Russian Cup, organized by the Skolkovo Foundation. The Skolkovo Foundation runs the Skolkovo Innovation Center, a Moscow business

[332] It lists one single-authored paper, titled "Static Dalvik VM bytecode instrumentation," from June 2017 that "proposes a novel approach to restricting the access for blacklisted Android system API calls. Eugene Minibaev, "Static Dalvik VM bytecode instrumentation," *Research Gate*, (June 2017), .

[333] Eugene Minibaev, « Предметно-ориентированный отладчик для системы динамической двоичной трансляции QEMU », *Research Gate*, (April 2019).

and technology hub started by then-president Dmitri Medvedev in 2010.[334] While it was meant to serve as a type of Russian Silicon Valley, corruption, brain drain problems, and Putin's Internet crackdown later ground the project to a halt[335]—though, the Foundation still touts that hundreds of industrial partners, professors, and students participate in the hub.[336]

Teams are composed of a captain, programmer, web vulnerability expert, forensic expert, administrator, mathematician/cryptographer, and reverse engineer.[337] In 2019, the CTF Russian Cup organizers hosted 46 competitions in Russia in 20 different cities: Barnaul, Vladimir, Voronezh, Yekaterinburg, Zavodoukovsk, Innopolis, Korolev, Krasnodar, Krasnoyarsk, Makhachkala, Moscow, Novosibirsk, Omsk, Penza, St. Petersburg, Simferopol, Tomsk, Tyumen, Khabarovsk, and Khanty-Mansiysk.

Over 3,500 hackers participated of whom 140 participated in the final tournament. The competition includes challenges focused on using web vulnerabilities, steganography (hiding data with an ordinary-looking message), and scraping open-source information.[338]

The competition brings in judges from across the Russian private sector, including those working at companies supporting the Russian intelligence community. Previous judges for the Skolkovo CTF and the related Skolkovo Cybersecurity Challenge have included:

- Alexander Budnikov, a member of the Russian Academy of Cryptography and the chief information officer (previously the managing director for information security) at publicly traded Russian conglomerate AFK Sistema.
- Ilya Derlysh, the head of information security and special projects at Kronstadt Unmanned, part of the U.S.- and UK-sanctioned Kronstadt Group that supplies unmanned aerial systems and weaponry to the Russian military.[339]

---

[334] See, e.g., Peter Henderson, "Russian president downloads Silicon Valley success," *Reuters*, (June 23, 2010), https://www.reuters.com/article/oukin-uk-usa-politics-russia/russian-president-downloads-silicon-valley-success-idUKTRE65M50920100624.

[335] James Appell, "The Short Life and Speedy Death of Russia's Silicon Valley," *Foreign Policy*, (May 6, 2015), https://foreignpolicy.com/2015/05/06/the-short-life-and-speedy-death-of-russias-silicon-valley-medvedev-go-russia-skolkovo/; Ivan Nechepurenko, "Skolkovo Office Searched in Corruption Probe," *The Moscow Times*, (April 18, 2013), https://www.themoscowtimes.com/2013/04/18/skolkovo-office-searched-in-corruption-probe-a23399.

[336] « Фонда «Сколково» », *sk.ru*, (accessed October 3, 2022), https://sk.ru.

[337] "CTF Russian Cup," *cyberday.sk.ru*, (accessed October 3, 2022), https://cyberday.sk.ru/en/ctf-russian-cup/.

[338] In the competition, there are three kinds of final round tasks: task-based, attack-based, and penetration testing.

[339] Department of the Treasury, "U.S. Treasury Sanctions Russia's Defense-Industrial Base, the Russian Duma and Its Members, and Sberbank CEO," *Treasury.gov*, (March 24, 2022), https://home.treasury.gov/news/press-releases/jy0677; "Britain imposes sanctions on Russian drone manufacturer Kronstadt," *India Today*, (March 26, 2022), https://www.indiatoday.in/world/russia-ukraine-war/story/britain-impose-sanction-on-russian-drone-manufacturer-1929797-2022-03-26.

- Dmitry Sklyarov, the head of the application research department at Positive Technologies, the U.S.-sanctioned cybersecurity company that supports Russian intelligence community cyber operations. In July 2001, the United States arrested Sklyarov while visiting Las Vegas for his creation and publication of software to circumvent protections on copyrighted material under the U.S. Digital Millennium Copyright Act (DMCA) and helping his then-employer, Elcom Ltd, to do so.[340] In exchange for cooperation with the U.S. government, he returned to Russia. The Russian government refused to investigate his activities because, according to state media, his actions were not illegal under Russian law.[341]
- Ekaterina Starostina, a consultant for the Bank of Russia.
- Andrey Masalovic, the CEO of Lavina Puls.
- Vladimir Yeliseyev, the CEO of the Research and Advanced Developments Center for JSC InfoTeCS, otherwise known as "Infotecs," the U.S.-sanctioned, Russian cybersecurity company in January 2022 for enabling the activities of malicious Russian cyber actors.
- Natalia Kasperskaya, president of the InfoWatch group and former co-founder and CEO of Kaspersky Lab.
- Alexander Golubev, director of information security at PJSC VimpelCom, one of the largest telecommunications companies in Russia.
- Vitaly Zadorozhny, the chief information officer at U.S.-sanctioned bank Alfa-Bank and the former director of the cybersecurity lab at U.S.-sanctioned bank Sberbank.[342]

Skylarov offers an interesting case study. The U.S. government had him in custody two decades ago. Yet, once he cooperated with the investigation into his and his employer's criminal activity, he returned to Russia where he now leads a research arm of a company sanctioned for supporting the cyber operations and capability development of the Russian intelligence community. He also is active in the CTF competitions that build up the Russian cybersecurity talent base. The FSB, GRU, and other security organs recruit their own hackers at such events.

[340] Electronic Frontier Foundation, "US v. ElcomSoft Sklyarov," *eff.org,* (accessed October 3, 2022), https://www.eff.org/cases/us-v-elcomsoft-sklyarov. See *United States v. Elcomsoft* (01-cr-20138)(USDC, NDCA, 2002)

[341] « В России программисту Склярову уголовное дело не грозит », *RBC*, (August 9, 2001), https://www.rbc.ru/society/09/08/2001/5703b36f9a7947783a5a2b58. Sklyarov has also conducted research on vulnerabilities in major computer systems, such as identifying a vulnerability in 2021 in Intel's Atom, Celeron, and Pentium chips that allowed an unauthenticated user to active a test or debug mode—potentially allowing them to extract a computer's encryption key and access sensitive information stored on it. See also, Thomas Claburn, "Intel's recent Atom, Celeron, Pentium chips can be lulled into a debug mode, potentially revealing system secrets," *The Register*, (November 16, 2021), https://www.theregister.com/2021/11/16/intels_chip_flaw/

[342] Department of the Treasury, "Treasury Escalates Sanctions on Russia for Its Atrocities in Ukraine," *Treasury.gov*, April 6, 2022, https://home.treasury.gov/news/press-releases/jy0705.

There are other CTFs in Russia, though it is unclear if they are used by the intelligence community for recruitment, and if so, how much.

Case Study: State Recruitment from the Positive Hack Days Conference (PHDays)

Positive Technologies, which supports the Russian intelligence community's cyber operations, hosts events that the FSB and GRU use as recruiting events. One such suspected conference is the annual PHDays conference held in Moscow since 2011.

The current sponsors cover a range of Russian technology organizations, including companies that support the Russian government and defense complex, partner with companies like Positive Technologies, and offer services to help companies switch from foreign to domestic, Russian software and hardware:

Organization Title	How PHDays Describes its CTF Role	Description of Organization
Innostage	Co-organizer	Russian IT and cybersecurity company servicing large Russian enterprises and state organizations, like Rosneft;[343] its founder has publicly expressed support for Moscow blocking access to Twitter and other sites[344]
Security Vision	Business Partner	Russian cybersecurity company focused on security operations centers (SOCs), incident response, and security intelligence;[345] it built a situational information security center for state defense conglomerate Rostec and works on numerous other projects for government agencies[346]
Mont	Business Partner, Exhibition Participant	Russian software distribution company[347]
Rostelecom Solar	Business Partner	Russia's state-owned telecom
Azbuka Vkusa	Technological Partner	Russian supermarket chain[348]
InfoWatch	Partner, Exhibition Participant	Russian cybersecurity company specializing in data loss prevention, among others; it was founded as a Kaspersky Lab subsidiary in 2003 focused on

[343] « ГК Innostage — Клиенты », innostage-group.ru, (accessed September 27, 2022), https://www.innostage-group.ru/clients/.

[344] "Aydar Guzairov: 'The task of sovereign internet can be solved no earlier than in two years in Russia,'" *Realnoe Vremya*, (March 17, 2021), https://realnoevremya.com/articles/5325-the-task-of-sovereign-internet-can-be-solved-no-earlier-than-in-2-years.

[345] "Security Intelligence LLC," *securityvision.ru*, (accessed September 27, 2022), https://www.securityvision.ru/en/vendor/.

[346] "Projects – Government," *securityvision.ru*, (accessed September 27, 2022), https://www.securityvision.ru/en/projects/index.php?client_type=Government&product_type=vse_produkty.

[347] "MONT," *mont.com*, (accessed September 27, 2022), https://mont.com.

[348] « Азбука вкуса », *av.ru*, (accessed September 28, 2022), https://av.ru.

		protecting against leaks of confidential information and was spun out in mid-2012[349]
Jet Infosystems	Partner, Exhibition Participant	Russian IT system integration company[350]
Axoft	Partner, Exhibition Participant	Russian IT software distributor servicing Russia and the Commonwealth of Independent States (Azerbaijan, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, and Ukraine); official software distributor for Kaspersky Lab, Positive Technologies, and other Russian firms as well as Red Hat, Hewlett Packard Enterprise, and other Western companies;[351] it has worked with Kaspersky for over 15 years[352]
Fortis	Partner, Exhibition Participant	Russian information security, network, and cloud technology company operating in Russia, Hungary, Romania, Kazakhstan, Uzbekistan, and Kyrgyzstan[353]
R-Vision	Exhibition Partner	Russian cybersecurity company that offers continuous monitoring, cyber intrusion simulations, and other services;[354] its clients include state-controlled pipeline transport company Transneft, Gazprom subsidiary and regional power generation company Mosenergo, and numerous government agencies including the Federal Financial Monitoring Service (Росфинмониторинг); Federal Customs Service; Ministry of Digital Development, Communications, and Mass Media (which houses Роскомнадзор, the Russian internet and media censor); the Mayor of Moscow's office; the Russian Federation Pension Fund; and the Federal Tax Service; it also services clients in CIS countries and Russian state media like RIA[355]

[349] "Kaspersky Lab and InfoWatch Become Independent from Each Other," *Kaspersky.com*, (May 17, 2012), https://www.kaspersky.com/about/press-releases/2012_kaspersky-lab-and-infowatch-become-independent-from-each-other.

[350] "About Us," *jetinfosystems.com*, (accessed September 29, 2022), https://jetinfosystems.com/about/.

[351] "Partner Details: Axoft JSC," *partners.fireeye.com*, (accessed September 29, 2022), https://partners.fireeye.com/directory/partner/367930/axoft-jsc; axoftglobal.ru, accessed September 29, 2022, https://axoftglobal.ru.

[352] Axoft, "Kaspersky and Axoft expand cooperation to drive Enterprise business growth in Turkey," *tr.axoftglobal.com*, (September 20, 2021), https://tr.axoftglobal.com/kaspersky_press-release. Interestingly, the current commercial director for Kaspersky Lab, who works on corporate relations, sales, business-to-business, and marketing, was previously the CEO of Axoft in Kyrgyzstan.

[353] *fortis-distribution.com*, (accessed September 29, 2022), https://fortis-distribution.com/index.php/en/.

[354] "R-Vision SENSE," *rvision.ru*, (accessed September 29, 2022), https://rvision.ru/products/sense; "R-Vision TDP," rvision.ru, accessed September 29, 2022, https://rvision.ru/products/tdp.

[355] « Клиенты », *rvision.ru*, (accessed September 29, 2022), https://rvision.ru/clients.

Marvel Distribution	Partner, Exhibition Participant	Russian IT distribution company operating in Russia and CIS countries[356]
Pangeo Radar	Partner	Russian information security software company focused SOC automation[357]
Liberum Navitas	Partner, Exhibition Participant	Russian IT outsourcing company that offers data centers, public cloud services, and private cloud services;[358] it is currently building a cross-Russia network of 15 data centers, mostly sourcing domestic hardware and software[359]
Gazinformservice	Partner	Russian cybersecurity company focused on workstation and IT infrastructure protection;[360] its partners include Huawei, Kaspersky, InfoWatch (described above), Infotecs (the Moscow CTF sponsor sanctioned by the U.S. for supporting Russian intelligence community cyber operations), Positive Technologies (the U.S.-sanctioned company also supporting Russian intelligence community cyber operations), and Lenovo, among others[361]; it also cooperates with Russian universities to train students in cybersecurity and specifically advertises services to help companies transition from foreign to domestic Russian database management systems[362]
IBS Platformix	Partner, Exhibition Participant	Russian IT company that provides data storage, control systems for IT infrastructure, and more;[363] its partners include Astra Linux, Check Point, Fortinet, Group-IB, Huawei, InfoWatch, Kaspersky, Palo Alto Networks, Positive Technologies, Symantec, Infotecs, and Gazinformservice;[364] it is a subsidiary of Russian

[356] "Marvel-Distribution," *marvel.ru*, (accessed September 29, 2022), https://www.marvel.ru/en/.

[357] « О компании », *pangeoradar.ru*, (accessed October 1, 2022), https://pangeoradar.ru/pages/about-company.

[358] « Наши услуги », *liberumnavitas.com*, (accessed October 1, 2022), http://www.liberumnavitas.com.

[359] Dan Swinhoe, "Liberum Navitas launches project to build network of 15 data centers across Russia," *datacenterdynamics.com*, (October 21, 2021), https://www.datacenterdynamics.com/en/news/liberum-navitas-launches-project-to-build-network-of-15-data-centers-across-russia/; Dan Swinhoe, "Russian operation Liberum Navitas chooses locations for first three of 15 data centers," *datacenterdynamics.com*, (February 28, 2022), https://www.datacenterdynamics.com/en/news/russian-operator-liberum-navitas-chooses-locations-for-first-three-of-15-data-centers/.

[360] "Gazinformservice," *crunchbase.com*, (accessed October 1, 2022), https://www.crunchbase.com/organization/gazinformservice.

[361] « Партнеры », *gaz-is.ru*, (accessed October 1, 2022), https://www.gaz-is.ru/o-kompanii/vendory.html.

[362] « ГИС, УРФУ и СПбПУ обсудили партнерство в образовании », *it-world.ru*, December 20, 2021, https://www.it-world.ru/news-company/events/180797.html; « Чем заменить иностранную СУБД? », *it-world.ru*, (May 31, 2022), https://www.it-world.ru/cionews/business/184919.html.

[363] *platformix.ru*, (accessed October 1, 2022), https://platformix.ru.

[364] « Партнеры », *platformix.ru*, (accessed October 1, 2022), https://platformix.ru/about/partner.

		IT giant IBS, which has faced market volatility since 2018 due to U.S. sanctions and whose founder, Anatoly Karachinsky, was sanctioned by the U.S. in April 2022 for ties to a Russian state bank[365]
USSC	Partner	Russian IT modernization and cybersecurity company; services 250 of the largest Russian enterprises;[366] it runs an important substitution service to switch clients over to domestic hardware and software;[367] its partners include Huawei, Infotecs, InfoWatch, and Positive Technologies[368]
Atom Security (StaffCop)	Partner	Russian endpoint security company[369]

Positive Hack Days is a significant recruiting event for the FSB and GRU. For example, in 2017, one of the attendees was Anatoliy Sergeyevich Kovalev, whose affiliation was listed as Moscow State Technical University.[370] A journalist uncovered that, while there is a professor at the university with the same first and last name, the professor's patronymic is different. But the name exactly matches a GRU Unit 74455 ("Fancy Bear") hacker indicted by the United States for developing spearphishing techniques and messages that the GRU used to target *En Marche!* officials, employees of the UK's Defense Science and Technology Laboratory (DSTL), members of the International Olympic Committee and Olympic athletes, and a media entity in Georgia.[371]

[365] Henry Foy, "Russian IT firm IBS freezes planned IPO amid sanctions uncertainty," *Financial Times*, (April 13, 2018), https://www.ft.com/content/1d678022-3f28-11e8-b9f9-de94fa33a81e; "Karachinsky ceases being owner of IBS holding company, stake transferred to management," *Interfax*, (June 2, 2022), https://interfax.com/newsroom/top-stories/79788/; Department of the Treasury, "Russia-related Designations and Designation Update; Issuance of Russia-related General Licenses," *treasury.gov*, (April 20, 2022), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220420; "Public Joint-Stock Company Bank Otkritie Financial Corporation," *fitchratings.com*, (August 9, 2021), https://www.fitchratings.com/research/banks/public-joint-stock-company-bank-otkritie-financial-corporation-09-08-2021.

[366] « О компании », *career.ussc.ru*, (accessed October 1, 2022), https://career.ussc.ru/company/index.php.

[367] « Импортозамещение », *ussc.ru*, (accessed October 1, 2022), https://www.ussc.ru/product/importozameshchenie/.

[368] « Партнеры УЦСБ », *ussc.ru*, (accessed October 1, 2022), https://www.ussc.ru/company/partners/.

[369] "Atom Security," *tracxn.com*, (accessed October 1, 2022), https://tracxn.com/d/companies/staffcop.com; "StaffCop," *staffcop.ru*, (accessed October 1, 2022), https://www.staffcop.ru.

[370] Kevin Poulsen, "This Hacker Party Is Ground Zero for Russia's Cyberspies," *The Daily Beast*, (August 4, 2018), https://www.thedailybeast.com/this-hacker-party-is-ground-zero-for-russias-cyberspies-3.

[371] Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," *Justice.gov*, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-

Hence, this GRU hacker attends Positive Hack Days, ostensibly to meet participants and recruit them for the military intelligence agency. In 2014, Dmitry Sergeyevich Badin attended—an officer in GRU Unit 26165, a hacking unit that also travels abroad to hack targets on-site, and who was an assistant to Boris Antonov, the head of the GRU team that hacked the Democratic National Committee in 2016.[372] That same year, Russian hacker Alisa Andreevna Shevchenko attended Positive Hack Days and delivered a keynote; the U.S. government later sanctioned her company, ZOR Security, for providing "technical research and development" to the GRU in service of its interference in the 2016 U.S. election.[373]

The 2022 conference promised contests focused on ATM hacking, smart home technology, surveillance cameras, Internet of Things (IoT) devices, smart cars, and other technologies. It also had a central competition called The Standoff, which Positive Technologies described as "a 30-hour cyberbattle between teams of attackers, defenders, and security operations centers." In this simulation, according to Positive Technologies, the attackers launched attacks to stop oil production (at a fictional company that produces, refines, stores, and sells oil and gas), shut down an oil production pipeline, disrupt a water treatment facility, disrupt a Ferris wheel, and disrupt a jet bridge, among other targets. Participants dealt with attacks on a fictional banking system and with disruptions of a railway ticketing system.

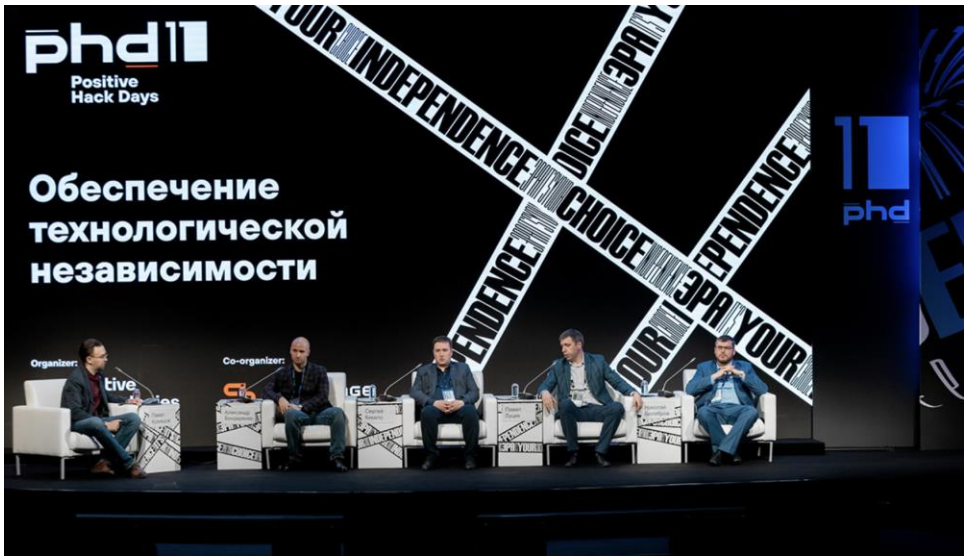


Photo released from Positive Hack Days 2022

deployment-destructive-malware-and. See *United States v. Andrienko, et al.* (20-cr-316)(USDC, WDPA)(October 2020).

[372] "Investigative Report: On The Trail Of The 12 Indicted Russian Intelligence Officers," RadioFreeEurope/RadioLiberty, July 19, 2018, https://www.rferl.org/a/investigative-report-on-the-trail-of-the-12-indicted-russian-intelligence-officers/29376821.html. See *United States v. Netyksho, et al.*, (18-cr-215)(USDC, DC, July 2018).

[373] Poulsen, "This Hacker Party Is Ground Zero for Russia's Cyberspies."

This year, PHDays also ran what it described as the first all-Russian open-source cybersecurity competition for children and students. Denis Korablev, Positive Technologies' product director, spoke about how the open-source community has come better to identify vulnerabilities and quantitatively improve products. He added that holding open-source cybersecurity competitions provides a way for young professionals to break into the cybersecurity community and discover opportunities. The competition solicited submissions on protecting against malicious code, detecting and preventing attacks, understanding cyber threats, and solving other urgent cybersecurity issues.

Oleg Skulkin, who runs digital forensics and incident response at Group-IB,a Singapore-based cybersecurity company that spun off a local Russian entity in July to stay in the Russian market,[374] attended the conference and said that, in recent months, the world's hacking community had come to see Russian companies as fair game. Other speakers talked about systematically engaging the Russian hacker community in protecting Russian computer systems; for example, the cybersecurity director for Russia's Ministry of Digital Development, Communications, and Mass Media spoke about expanding Russian bug bounty platforms, like Positive Technologies' The Standoff 365 Bug Bounty. There were other presentations on detecting attacks, scoring indicators of compromise, sanitizing the Linux kernel, and using open-source intelligence.[375]

Participation in the PHDays conference has steadily increased over the last decade, with the exception of 2020, when no conference was held, and in 2021, when there was a dip in attendance. The cause is unclear, but it is plausible that attendance fell because there was no conference in 2020 and because Russia was still reeling from the coronavirus.

Year	Participants	Talks	Hands-on Labs	Contests
2011	500	35	10	8
2012	1,500	62	10	19
2013	2,200	65	9	15
2014	2,500	65	5	10
2015	3,500	60	6	15
2016	4,200	75	8	12
2017	6,000+	85	7	14
2018	5,200+	100	5	14
2019	8,000+	100+	6	13
2020	n/a	n/a	n/a	n/a

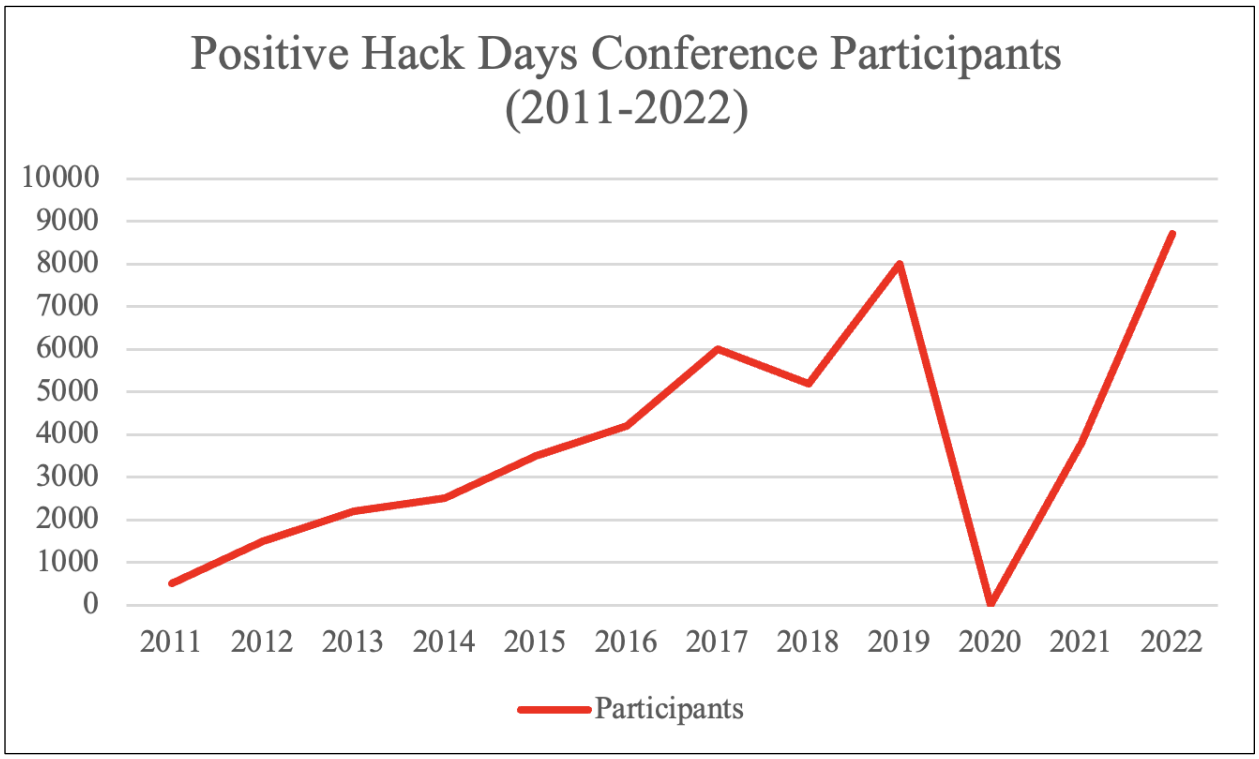
[374] "Cyber firm Group-IB to split Russian, international businesses," *Reuters*, (July 6, 2022), .

[375] "PHDays 11 talks: bootkit infection, sanitizers for the Linux kernel, the new face of OSINT, and phishing on official websites," phdays.com, April 29, 2022, https://www.phdays.com/en/press/news/phdays-11-talks/.

2021	3,800	74	17	6
2022	8,700	100	unknown	unknown

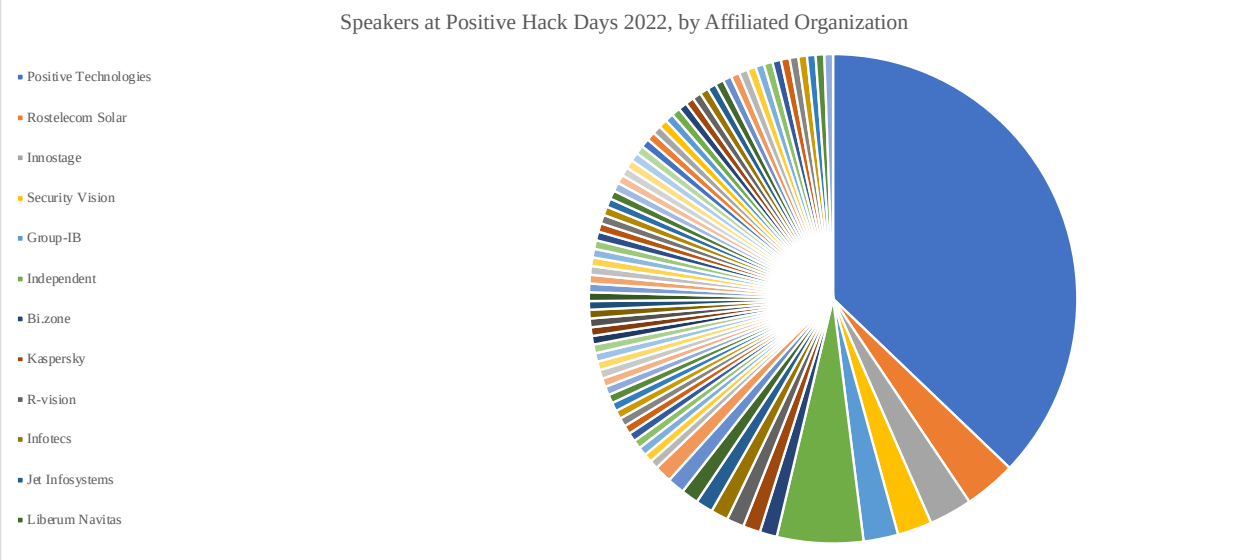
Positive Hack Days Statistics (2011-2022)

Positive Hack Days has become an increasingly popular event for the Russian cybersecurity community, beginning with just 500 participants in 2011 to the most recent, 2022 conference hosting 8,700 people on-site in Moscow. This coincides with the U.S. government publicly disclosing that the FSB and GRU leverage Positive Technologies-run events to recruit hackers to work for the Russian government.



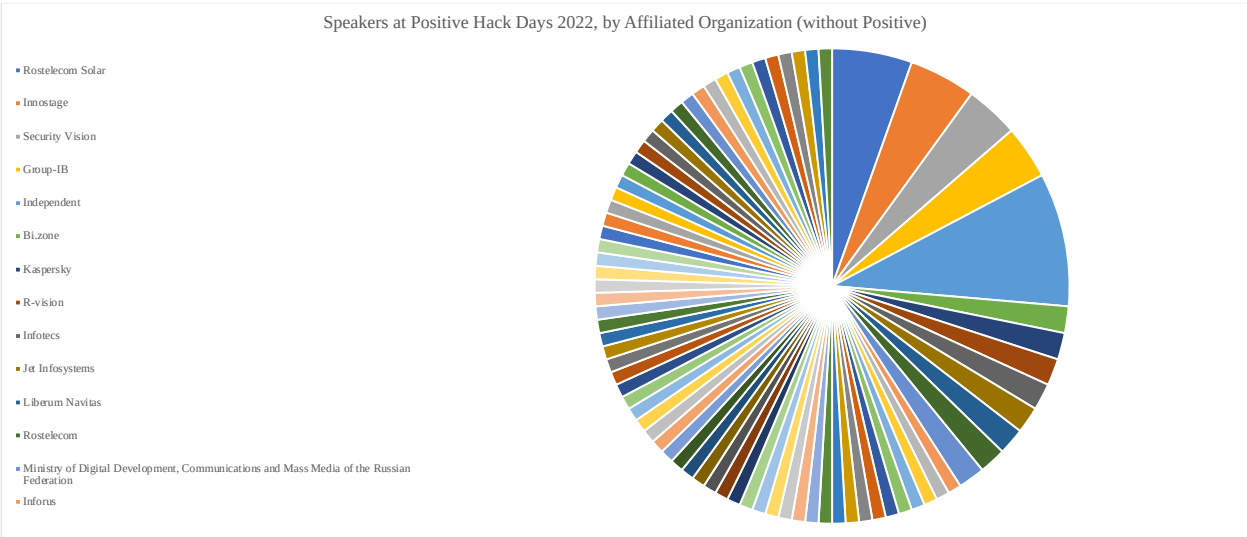
PHDays Conference Participants

The 2022 conference speakers were composed predominantly of participants from Positive Technologies. Out of the 175 identified conference speakers, many came from just a few cybersecurity companies: 65 from Positive Technologies, 6 from Rostelecom Solar, 5 from Innostage, 4 from Security Vision, and 4 from Group-IB. Speakers were also present from Kaspersky Labs, Jet Infosystems, Inforus, InfoWatch, and Yandex Cloud, among other Russian cybersecurity and technology companies. There were two speakers from Rostelecom (the Russian state-owned telecommunications provider), two speakers from the Russian Ministry of Digital Development, Communications, and Mass Media, and one speaker from the Mozhaisky Military Space Academy.



Speakers at Positive Hack Days 2022, by Affiliated Organization

Removing the Positive Technologies speakers from the dataset highlights a wide range of Russian cybersecurity and technology companies, as well as government and academic organizations, represented at the conference.



Speakers at Positive Hack Days 2022, by Affiliated Organization (without Positive)

Maxut Shadayev, the Russian minister of Digital Development, Communications, and Mass Media was one of these speakers. His previous positions include the assistant to the head of the Russian Presidential Executive Office (2008-2009), the vice president for digital platforms at Rostelecom (2018-2019), and the director general of RT Labs, a subsidiary of Rostelecom that

works on large infrastructure projects for government and corporate clients (also in 2019).[376] While at the Presidential Executive Office, Shadayev also previously oversaw the work of the Russian Presidential Council for Information Society Development chaired by then-Russian president Dmitry Medvedev.

Later, in 2017, Putin would sign an executive order on the Strategy for the Development of an Information Society in the Russian Federation,[377] focused on safeguarding the information sphere—in other words, controlling the information space.[378] Shadayev now oversees the ministry responsible for controlling media in Russia and censoring the internet, among other functions.[379]

In another one of the most notable appearances, Maria Zakharova, the spokesperson for Russia's Ministry of Foreign Affairs, gave a presentation alongside Vladimir Zopolyansky, the chief marketing officer of Positive Technologies. Zakharova has been dubbed Russia's "troll-in-chief"[380] and is one of the Kremlin's and Putin's most prominent spokespeople in the global media. She frequently appears on Russian television, gives many press briefings, and provides comments to numerous Russian online media outlets that parrot state talking points.

In recent years, Zakharova has called U.S. journalists anti-Russian propagandists, repeated conspiracy theories that the United States is developing biological weapons in third countries, lied (pre-February invasion) that NATO was sending militants to Ukraine, and called Russia's repressive "foreign agent" law an "eye-for-an-eye" response to Western interference.[381]

---

[376] Government of the Russian Federation, "Maksut Shadayev," *government.ru*, (accessed October 14, 2022), http://government.ru/en/gov/persons/627/events/; "RT Labs," *tadviser.com*, (accessed October 14, 2022), https://tadviser.com/index.php/Company:RT_Labs.

[377] "Strategy for Information Society Development until 2030 approved," *kremlin.ru*, (May 10, 2017), http://en.kremlin.ru/acts/news/54477; « Указ Президента Российской Федерации от 09.05.2017 г. № 203 », *kremlin.ru*, (September 5, 2017), http://kremlin.ru/acts/bank/41919.

[378] Marta Kowalska, *Analysis of the Russian 'Strategy for the Development of an Information Society,'* (Warsaw: Center for Propaganda and Disinformation Analysis, May 25, 2017), https://capd.pl/en/analyses/185-analysis-of-the-russian-strategy-for-the-development-of-an-information-society.

[379] Shadayev took over the minister position in January 2020. In November 2020, Putin abolished Rospechat (the Federal Agency for Press and Mass Media) and Rossvyaz (the Federal Communications Agency), two other key agencies in domestic technology development and media control, and moved their functions to the Ministry of Digital Development, Communications, and Mass Media. At the time, the Ministry already housed Roskomnadzor, Russia's internet and media censor. See: "Putin abolishes Rospechat, Rossvyaz, assigns their duties to Ministry of Digital Development, Communications and Mass Media," *Interfax*, (November 20, 2020), https://interfax.com/newsroom/top-stories/70411/.

[380] Konstantin Benyumov and Emily Tamkin, "Meet The Woman Who Is Proudly Russia's Troll-In-Chief," *BuzzFeed News*, (October 22, 2018), https://www.buzzfeednews.com/article/konstantinbenyumov/maria-zakharokva-profile-russian-foreign-ministry.

[381] "US media should apologize for two years of anti-Russian propaganda — Foreign Ministry," *TASS*, (March 26, 2019), https://tass.com/world/1050665; "US labs in third countries may be developing pathogenic agents — diplomat," *TASS*, (April 17, 2020), https://tass.com/politics/1146327; "NATO

In May 2022, Zopolyansky called her conference talk with Positive Technologies "Creating a Multipolar World." It focused on the concept of "digital independence and digital sovereignty," a notion of growing importance to the Kremlin amid Western technology sanctions and the Russian government's continued push to exert "cyber sovereignty," (e.g., control the internet and information space) within its own borders. It was notable that Positive Technologies' chief marketing officer presented this speech alongside a Kremlin spokesperson on the podium. Zakharova's attendance would have been noteworthy in any event. It indicated Russian official interest in the conference and the cultivation of a pro-regime hacker community.

Case Study: The Russian Hacker Community at the Offzone Conference

Offzone is an international cybersecurity conference held in Moscow since 2018. Its partners are cybersecurity companies Bi.ZONE, Positive Technologies, Angara Security, Kaspersky, Security Code, DeteAct, Swordfish Security, Servicepipe, and ICL; Russian bank Sberbank; financial technology company Sovcombank; cybersecurity educational center CyberEd; e-ticket company Timepad; and the Digital Economy League, a professional services company with clients that include Sberbank, Rostelecom, Alfa-Bank, Rosneft, and numerous other Russian state institutions and companies.[382]

Interestingly, the English-language version of the website stops there. The Russian-language version of the website lists another sponsor, RTK-Solar, otherwise known as Rostelecom Solar, the Russian cybersecurity company.[383]

From 2018 to 2019, the conference doubled in size. There are no attendance data available on 2020, 2021, or 2022 as the 2022 conference took place in August 2022.

Year	Attendees	Experts (Speakers)	Partners
2018	1,000	52	8
2019	2,000	63	23
2020	Unknown	Unknown	Unknown
2021	Unknown	Unknown	Unknown
2022	Unknown	68	Unknown

Speakers at OffZone 2019, by Affiliated Organization

sending militants under guise of military instructor to Ukraine — Russian diplomat," *TASS*, (December 12, 2021), https://tass.com/russia/1374401; "Russian Spokeswoman Defends 'Foreign Agent' Law As 'An Eye-For-An-Eye' Reaction," *RadioFreeEurope/RadioLiberty*, (June 3, 2021), https://www.rferl.org/a/russia-foreign-agent-zakharova/31288588.html.

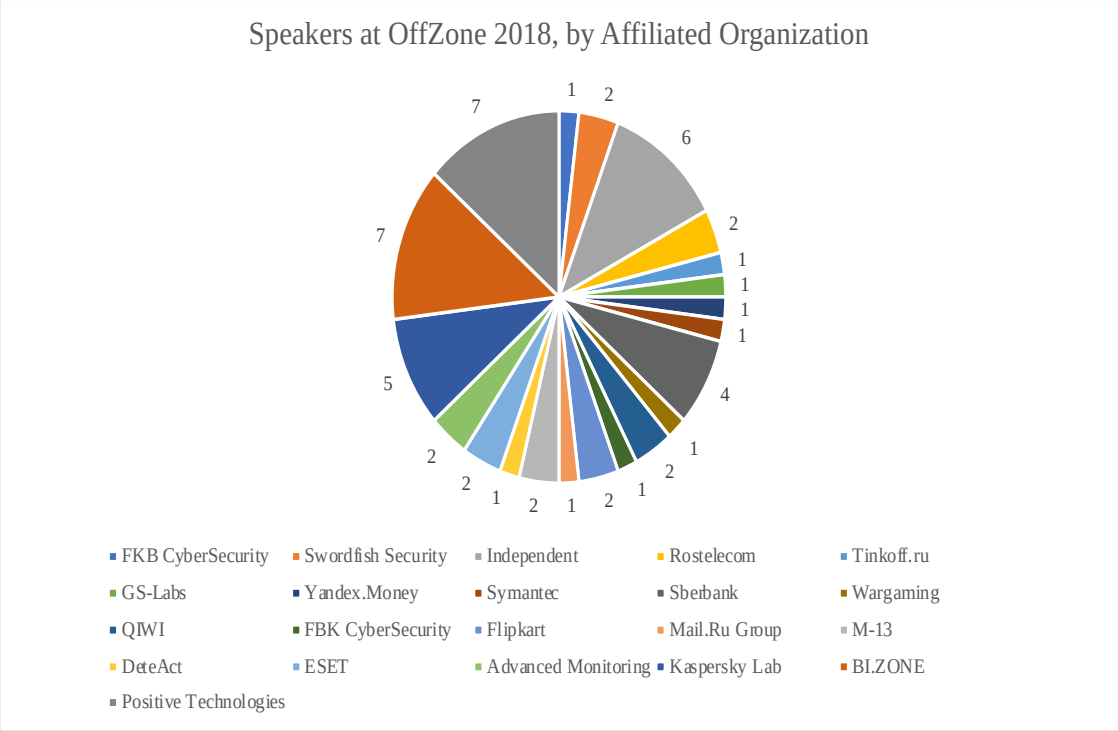
[382] "Sponsors and partners," *offzone.moscow*, (accessed October 14, 2022), https://offzone.moscow/sponsors-and-partners/.

[383] « Спонсоры и партнеры », *offzone.moscow*, (accessed October 14, 2022), https://offzone.moscow/ru/sponsors-and-partners/.

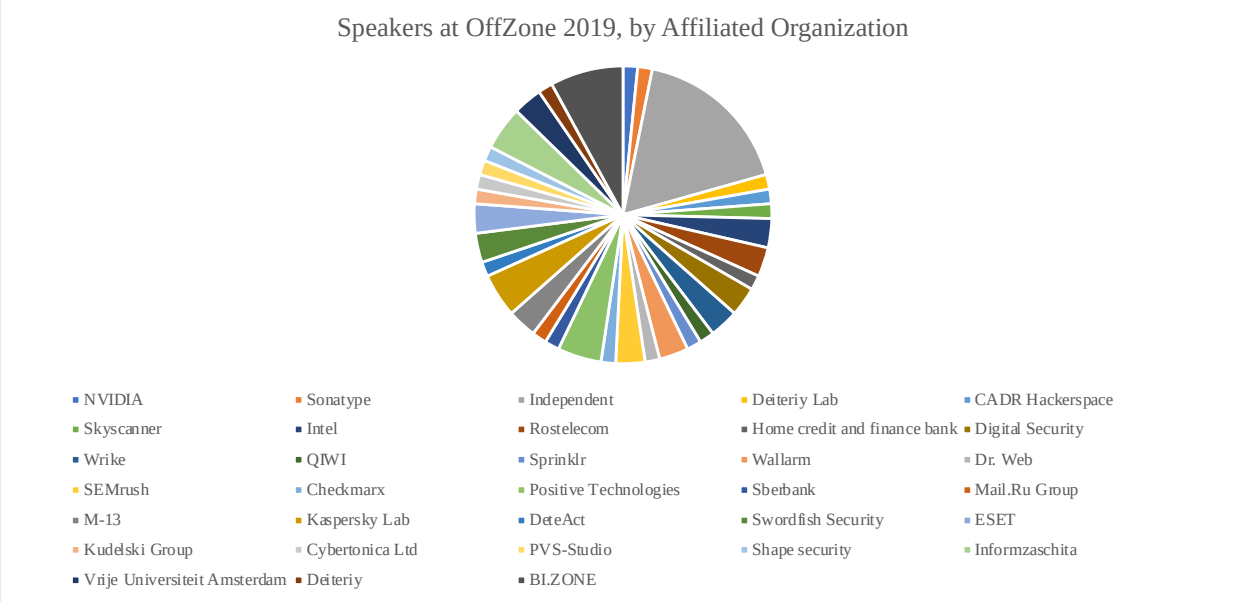
The OffZone speakers represent some of the key players in the Russian private-sector cybersecurity ecosystem. In 2018, cybersecurity companies Positive Technologies and Bi.Zone were most represented at the conference, with seven speakers each, following by unaffiliated independent security researchers and experts (six speakers) and people from Kaspersky Labs (five speakers). Someone from Symantec also spoke (one speaker).

In 2019, the most speakers were independent security researchers and experts (11) followed by people from Bi.Zone (five speakers), Positive Technologies (three speakers), *Informzaschita* (three speakers), and Kaspersky Labs (three speakers). Someone from NVIDIA also spoke in 2019 (one speaker).

There is no information available on the 2020 and 2021 conference, though ostensibly the 2020 conference was not held due to Covid-19. For 2022, the most speakers were independent security researchers and experts (12) followed by speakers from Positive Technologies (six speakers), Sber (four speakers), and companies like Kaspersky (three speakers), Deiteriy (three speakers), Jet Infosystems, and Innostage (two speakers). The data on the 2018, 2019, and 2022 conference speakers are displayed below.



Speakers at OffZone 2018, By Affiliated Organization



Speakers at OffZone 2019, By Affiliated Organization

Speakers at OffZone 2022, By Affiliated Organization

In 2018 and 2019, the conference was host to a capture the flag competition, dubbed CTFZONE. The top ten qualified teams in 2018, selected from the CTFZONE tournament, competed at the Offzone conference, coming from Russia, Hungary, Poland, South Korea, Ukraine, and China.[384]

[384] "CTFZONE 2018," *2018.offzone.moscow*, 2018, https://2018.offzone.moscow/ctfzone/.

2018 CTFZONE Finalist Name	Team Country
LC↯BC	Russia
!SpamAndHex	Hungary
p4	Poland
Bushwackers	Russia
GoGiSaJo	South Korea
LeaveCat	South Korea
CyKor	South Korea
dcua	Ukraine
Dragon Sector	Poland
0ops	China

Growing Brain-Drain Challenges

Since the fall of the Soviet Union, highly skilled scientists, technology experts, and other well-educated Russians emigrated. Some were aiming for freer and more profitable lives in Western countries. Others may have sold their skills to the highest bidder, whoever that might be, and to serve whatever purpose the payer might have. Still others may have emigrated for religious or ethnic reasons, moving to countries with which they had or thought they had affinities.[385] The return of political repression under Putin caused another wave of emigration by professionals and others.

A brain drain featured in and perhaps contributed to the Soviet collapse. Between 1983 and 1993, many of the 218,000-plus Russian citizens who emigrated to the United States were highly educated in fields such as physics, law, engineering, and computer science. They seem to have been motivated by the wish for stable employment and political freedom.[386] In the second half of the 1990s, labor conditions and ethnic issues drove emigration.[387]

At the time, CIA worried about this brain drain from a national and international security perspective. Then-Director Robert Gates testified in 1992 that some of the Soviet scientists with nuclear weapons design skills could travel to other countries or even sell information.[388] At least

[385] Erik Volz, "*Utechka Umov*: The History, Implications, and Solutions Concerning Russia's Post-Soviet Brain Drain," *jur* (Fall 2002): 35-40, 36.

[386] See, e.g., Suzanne Possehl, "Russian Brain Drain Flows Directly Into U.S. Science Talent Reservoir," *Los Angeles Times*, (February 26, 1995), https://www.latimes.com/archives/la-xpm-1995-02-26-mn-38775-story.html.

[387] Andrei V. Korobkov and Zhanna A. Zaionchkovskaia, "Russian brain drain: Myths v. reality," *Communist and Post-Communist Studies*, (September/December 2012): 327-341, 328.

[388] R. Jeffry Smith, "Gates Fear Soviet 'Brain Drain,'" *The Washington Post*, (January 16, 1992), https://www.washingtonpost.com/archive/politics/1992/01/16/gates-fears-soviet-brain-drain/7a0038c2-

one analyst argues this was not a "mass exodus" driven by political and religious persecution as was seen at various times in the nineteenth and twentieth centuries. Rather, a global, scientific job market fueled emigration. In the Soviet Union's case, *perestroika* policies, a lack of opportunity, and other factors drove talented Russian scientists and engineers out of the country.[389] Former Soviet president Mikhail Gorbachev himself told Henry Kissinger in 1989 that "as far as the dissidents are concerned, let them all go to your country" but that he would "fight against the brain drain."[390]

Loss of intellectual talent has proved to be a persistent and growing problem for the Putin regime. In 2004, a study of Moscow universities found Russian scholars and students' top emigration reasons were low wages (76% of respondents), a decline in the prestige of intellectual labor (53% of respondents), and a lack of opportunities to realize potential (50% of respondents).[391] From 1996 to 2020, another study found, scholars leaving Russia had more citations to them in professional journals than did those entering the country, with the most obvious brain drain in neuroscience, decision sciences, mathematics, biochemistry, and pharmacology.[392]

More recently, technology has seen talent loss. In 2018, the head of the Russian Academy of Sciences said the Russian government was too focused on dollars coming into and out of the Russian economy and not focused enough on the departures of technological talent.[393] During the Covid-19 pandemic, some observers feared that thousands more Russian IT personnel might leave the country.[394]

2fdf-47c6-bab7-9ac9af32fdc6/. Research suggests that immigration in other security-sensitive scientific fields was limited, as with chemical and biological weapons researchers. Shalkovskyi Volodymyr, *An Analysis of the Brain Drain Phenomenon in the Field of Development of Chemical and Biological Weapons in Russia During the 1990s* (Monterey: U.S. Naval Postgraduate School, June 2002), https://apps.dtic.mil/sti/citations/ADA406045.

[389] R. Adam Moody, "Reexamining Brain Drain from the Former Soviet Union," *The Nonproliferation Review* (Spring/Summer 1996): 92-97, https://www.nonproliferation.org/wp-content/uploads/npr/moody33.pdf, 93.

[390] Henry Kissinger, *Conversation with Mikhail Gorbachev*, January 17, 1989, trans. Svetlana Savranskaya, Notes of A. S. Chernyaev, Archive of the Gorbachev Foundation, Cold War International History Project, https://chnm.gmu.edu/1989/items/show/141.html. See also Abraham R. Wagner, *Henry Kissinger: Pragmatic Statesman in Hostile Times* (New York: Routledge, 2020).

[391] Irina Ivakhnyuk, *Brain Drain from Russia: in Search for a Solution* (Warsaw: Centre for International Relations, 2006), http://pdc.ceu.hu/archive/00004817/01/rap_i_an_1506a.pdf, 4.

[392] Alexander Subbotin and Samin Aref, "Brain drain and brain gain in Russia: Analyzing international migration of researchers by discipline using Scopus bibliometric data 1996-2020," *Scientometrics* (2021): 7875-7900.

[393] « Глава Академии наук призвал отменить ЕГЭ », *RBC*, (April 3, 2018), .

[394] Vladimir Kozlov, "Russian Tech Industry Faces Coronavirus Brain Drain," *The Moscow Times*, June 17, 2020, https://www.themoscowtimes.com/2020/06/17/russian-tech-industry-faces-coronavirus-brain-drain-a70607.

Since Putin launched the war on Ukraine in February 2022, reports reveal that at least 70,000, and quite possibly more than 100,000 technology workers have fled Russia.[395] In March 2022, the Russian government announced that IT companies in Russia would receive a three-year income tax exemption as an incentive to stay in the country.[396]

Later in March 2022, the Russian government also announced it would exempt from mandatory military conscription male IT workers who are 27 years old or younger, hold a university degree, and have worked at a technology company for more than a year.[397] "It is important," said Russian Prime Minister Mikhail Mishustin, "not to allow the slowing down of the pace of development of the IT sector in our country even under sanctions."[398] The Russian government has also promised IT workers housing subsidies and salary increases.[399]

Most recently, the Russian government has exempted from conscription into the military people working at telecommunications companies, public communication facilities, data centers, the backbone of Russia's media ecosystem. Included here are the founders, editors, and publishers of registered TV and radio stations, as well as Russians working to keep the Russian financial market and payment ecosystem operating from military conscription.[400] These measures have not deterred many would-be emigrants. In fact, the Russian government has been weaponizing Russian data laws as a basis to expel nonprofits like the Jewish Agency for Israel, which helps Jewish people around the world emigrate to Israel, because Moscow believes it has been contributing to Russia's brain drain.[401]

There are many open questions about the nature and the future of this tech brain drain, including how it will affect Russia's open-source development community, the Russian government's talent recruitment, and Russian cybercrime as well as Russia's tech dependence on

[395] Yanina Sorokina, "Russia Plays Tug-of-War as Its Talented IT Workers Head for the Door," *The Moscow Times*, (April 19, 2022), https://www.themoscowtimes.com/2022/04/01/russia-plays-tug-of-war-as-its-talented-it-workers-head-for-the-door-a77160.

[396] "IT companies in Russia to be exempt from income tax for three years — PM," *TASS*, (March 2, 2022), https://tass.com/politics/1415189.

[397] "Russia 'Postpones' Military Service for IT Specialists," *Barron's*, (March 29, 2022), https://www.barrons.com/news/russia-postpones-military-service-for-it-specialists-01648544707.

[398] *Ibid*.

[399] Anthony Faiola, "Mass flight of tech workers turns Russian IT into another casualty of war," *The Washington Post*, (May 1, 2022), https://www.washingtonpost.com/world/2022/05/01/russia-tech-exodus-ukraine-war/.

[400] « Айтишники и связисты не подлежат мобилизации – Минобороны », *d-russia.ru*, (September 23, 2022), https://d-russia.ru/ajtishniki-i-svjazisty-ne-podlezhat-mobilizacii-minoborony.html.

[401] Justin Sherman, *Russia is weaponizing its data laws against foreign organizations*, (Washingon: Brookings Institution, September 27, 2022), https://www.brookings.edu/techstream/russia-is-weaponizing-its-data-laws-against-foreign-organizations/.

states like China.[402] It is also not guaranteed this phenomenon necessarily undermines the base of talent from which Moscow recruits uniformed state hackers. Hackers with a strong interest in military or intelligence service may not wish to leave the country for foreign research or private-sector jobs. The impact of accelerated IT brain drain therefore may fall heaviest on the non-governmental cyber community, which still plays a role in Moscow's offensive cyber activities but is not part of the uniformed services.

The trend is nonetheless worth watching as the Kremlin wages war on Ukraine and continues to try to expand its cyber and information operations capabilities. Western sanctions will continue to undermine Russia's economy,[403] and businesses continue to exit the market,[404] both of which contribute to a lack of opportunities for Russian programmers. On top of that, Putin continues to ramp up domestic repression[405] and make the political environment untenable for

[402] See, e.g., Gavin Wilde and Justin Sherman, *Putin's Internet Plan: Dependency with a Veneer of Sovereignty*, (Washington: Brookings Institution, May 11, 2022), https://www.brookings.edu/techstream/putins-internet-plan-dependency-with-a-veneer-of-sovereignty/.

[403] See, e.g., Alena Popova, *Tech Sanctions Against Russia Are Working*, (Washington: Center for European Policy Analysis, August 9, 2022), https://cepa.org/tech-sanctions-against-russia-are-working/; Anna Gross, "'Everything is gone': Russian business hit hard by tech sanctions," *Financial Times*, (June 2, 2022), https://www.ft.com/content/caf2cd3c-1f42-4e4a-b24b-c0ed803a6245; Ian Talley, "U.S. Sanctions Russian Tech Companies, Whole Sectors of Russian Economy," *The Wall Street Journal*, (March 31, 2022), https://www.wsj.com/articles/u-s-sanctions-russian-tech-companies-whole-sectors-of-russian-economy-11648748173; Jan Strupczewski, "Russia failing to by-pass sanctions on high-tech goods – U.S. official," *Reuters*, (September 2, 2022), https://www.reuters.com/world/europe/russia-failing-by-pass-sanctions-high-tech-goods-us-official-2022-09-02/; Jeffrey Sonnenfeld, et al., "Business Retreats and Sanctions Are Crippling the Russian Economy," *Social Science Research Network*, (July 20, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4167193.

[404] "Over 1,000 Companies Have Curtailed Operations in Russia — But Some Remain," *SOM.Yale.edu*, (accessed September 3, 2022), https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain. See also: "Companies Are Getting Out of Russia, Sometimes at a Cost," *The New York Times*, (August 25, 2022), https://www.nytimes.com/article/russia-invasion-companies.html; Carrie Mihalcik, Sarah Lord, and Corinne Reichert, "Companies That Have Left Russia: The List Across Tech, Entertainment, Finance, Sports," *CNET*, June 8, 2022, https://www.cnet.com/news/politics/companies-that-have-left-russia-the-list-across-tech-entertainment-finance-sports/.

[405] See, e.g., « После 24 февраля Кремль окончательно разгромил независимые СМИ в России. Но на их месте появляются новые », *Meduza*, (July 12, 2022), https://meduza.io/slides/posle-24-fevralya-kreml-okonchatelno-razgromil-nezavisimye-smi-v-rossii-no-na-ih-meste-poyavlyayutsya-novye; "Kremlin Pushes New Wave of Repression at Home as War Drags," *Bloomberg*, (July 6, 2022), https://www.bloomberg.com/news/articles/2022-07-06/kremlin-pushes-new-wave-of-repression-at-home-as-war-drags-on; Anton Troianovski and Valeriya Safronova, "Russia Takes Censorship to New Extremes, Stifling War Coverage," *The New York Times*, (March 4, 2022), https://www.nytimes.com/2022/03/04/world/europe/russia-censorship-media-crackdown.html; Irina Borogan, "Russian Special Services: From Political to Mass Repressions," *The Moscow Times*, (July 22, 2022), https://www.themoscowtimes.com/2022/07/22/russian-special-services-from-political-to-mass-repressions-a78384.

some highly educated individuals.[406] Foreign governments are targeting Russian IT talent outflows, too: Kazakhstan, for example, is providing loans and tax breaks to Russian tech entrepreneurs who relocate, and Uzbekistan has simplified its visa and residence permit process for tech professionals.[407]

[406] Emphasis on "some"—a recent poll from the independent Levada Center found that 45% of Russians think the Ukrainian regions of Kherson and Zaporizhzhia should be annexed and become part of Russia. "Levada Center: Almost half of Russians support annexing Ukraine's Kherson and Zaporizhzhia regions," *Meduza*, (September 2, 2022), https://meduza.io/en/news/2022/09/03/almost-half-of-russians-believe-russia-should-annex-ukraine-s-kherson-and-zaporizhzhia-regions.

[407] Niko Vorobyov, "'Criminal adventure': Ukraine war fuels Russia's brain drain," *Al Jazeera*, (May 23, 2022), https://www.aljazeera.com/news/2022/5/23/many-leave-russia-as-ukraine-war-drags-on.

5. Russian Open Source-Code

Open-source software (OSS) development solicits input from its community of users through technical standards meetings, code submissions, and online community discussions. These typically small communities are ripe targets for adversarial influence campaigns and software supply chain attacks.[408] There exists no established trust metric by which the open-source community can vet accounts or individuals that submit code based on code artifacts, commit quality, historic community influence, and affiliations. An attacker may contribute to popular libraries and submit deliberately vulnerable code or even functional backdoors that will be exploited after the code is incorporated into the product.

In addition, distracting core contributors, through useless change commits, flame wars such as hostile online comments or exchanges, or other activities, may lead to a failure to thoroughly vet patches or bug reports, leaving vulnerabilities in the code. Throughout all of this, Russia, a primary adversary in cyberspace, has expanded its focus on open-source software as a replacement for Western technology and as a means of expanding Russia's global technology footprint. This raises security risks for U.S. software.

Linux and Russia's Domestic Technology Push

The Russian government has recently accelerated its push to replace foreign technology with domestically made technology. Kremlin officials have instituted requirements for government organizations to transition to domestically produced software, developed tax incentives for companies producing domestic technology, and even increased their public speaking about the importance of domestic, Russian hardware and software. A key part of this push has been the Astra Linux operating system, built on Linux—which the Margin Research team, as part of its SocialCyber work, has examined at length.

Russian struggles with domestic technology are not new. In 1999, some of the key Russian research institutions received more than 25% of their funding from abroad.[409] Into the early 2010s, much Russian research and development in technology occurred in state-owned research institutes, "mostly separate from industrial firms and [higher educational institutions]."[410] The Russian government also continued to steal technology from the United States and the West. For example, in 2012, the Department of Justice indicted Alexander Fishenko, an unregistered Russian government agent living in the United States (known as an "illegal" operative), and 10 other

[408] Patrick Howell O'Neill, "The internet runs on free open-source software. Who pays to fix it?" *MIT Technology Review*, (December 17, 2021), https://www.technologyreview.com/2021/12/17/1042692/log4j-internet-open-source-hacking/.

[409] Loren Graham, "Science in the New Russia," *Issues* (Summer 2003), https://issues.org/graham-2/.

[410] *OECD Science, Technology, and Industry Outlook* (Paris: Organization for Economic Cooperation and Development, September 2012), https://www.oecd.org/sti/sti-outlook-2012-russian-federation.pdf, 368.

individuals and companies for operating a Russian military procurement network.[411] The individuals operated both in the United States and Russia to illegally procure high-tech microelectronics equipment on Moscow's behalf, which could be used in radar and surveillance systems, weapons guidance systems, as well as for detonation triggers for nuclear weapons.[412]

Around that time, the Russian government began focusing on barring the use of foreign technology from Russia. Decree No. 1236 in November 2015 provided that state organizations must purchase Russian software, except for when foreign software is the only kind of software that can satisfy the organization's requirements.[413] It also established a state registry for domestic, Russian-made software.[414] An investigation by Russia's Federation Council, the upper house of parliament, found some agencies were not following this law and buying Microsoft Windows anyway.[415]

By April 2016 the Russian government required all state-owned enterprises to have a government representative on the board responsible for domestic procurement.[416] Then, a few months later, the government required state-owned enterprises to vote on new company procurement policies for buying domestic Russian software.[417] As of May 2022, the Russian state registry lists more than 13,000 software products from 4,200 different organizations.[418]

Russia's focus on domestic software has ramped up since the 2015 and 2016 rules, and Linux has been a central part of the picture. In September 2017, Putin said that state institutions working with foreign technology could pose cybersecurity risks to Russia. "In terms of security," he said, "there are things that are critically important for the state, for sustaining life in certain

---

[411] Department of Justice, "Russian Agent and 10 Other Members of Procurement Network for Russian Military and Intelligence, Operating in the U.S. and Russia, Indicted," bis.doc.gov, (October 3, 2012), https://www.bis.doc.gov/index.php/all-articles/98-about-bis/newsroom/press-releases/press-releases-2012/447-russian-agent-and-10-other-members-of-procurement-network-for-russian-military-and-intelligence-operating-in-the-u-s-and-russia-indicted. See *United States v. Fishenko* (12-cr-626) (E.D.N.Y. July 29, 2013).

[412] *Ibid*.

[413] "Russian Federation: Banned purchase of foreign software in state and municipal orders," *Global Trade Alert*, (November 16, 2015), https://www.globaltradealert.org/state-act/10400/russian-federation-banned-purchase-of-foreign-software-in-state-and-municipal-orders.

[414] « Медведев запретил закупки иностранного ПО для нужд бюджетников », *Interfax*, (November 20, 2015), https://www.interfax.ru/business/480434.

[415] Andrei Zdanevich, "Why do Russians officials still prefer to use Microsoft?" *Russia Beyond*, (August 9, 2016), https://www.rbth.com/science_and_tech/2016/08/09/why-do-russian-officials-still-prefer-to-use-microsoft_619419.

[416] "Russia Expands Restrictions on Government Procurement of Foreign Software and Hardware," *jonesday.com*, (September 2016), https://www.jonesday.com/en/insights/2016/09/russia-expands-restrictions-on-government-procurement-of-foreign-software-and-hardware.

[417] *Ibid*.

[418] "Russian Ministry of Digital Development to transform domestic software register into marketplace," *Interfax*, (May 25, 2022), https://interfax.com/newsroom/top-stories/79526/.

sectors and regions."[419] Putin continued: "And if you are going to bring in hardware and software in such quantities, then in certain areas the state will inevitably say to you: 'You know, we cannot buy that, because somewhere a button will be pressed and here everything will go down.' So bear that in mind."[420]

Astra Linux is a variant of the Linux operating system built specifically for Russia over a decade ago.[421] In January 2018, the Russian government announced that it would deploy Astra Linux on all Russian military computers to replace Microsoft Windows, once the software met the proper security requirements.[422] Then, in April 2019, the Russian government certified Astra Linux to a "special importance" clearance level, meaning it was permitted to handle the most highly classified information and data from the Russian government.[423] Astra Linux is currently used by the Russian Ministry of Defense; the Ministry of Emergency Situations; the FSB; the state space company Roscomsos; and other state organizations.[424]

One of Russia's goals in using Astra Linux was the replacement of Microsoft Windows. Microsoft has had a storied history in Russia. In 2010, a journalist reported that Microsoft had given source code for Windows 7, Windows Server 2008 R2, Microsoft Office 2010, and Microsoft SQL Server to the FSB, as part of its Government Security Program to let governments access its source code.[425] Russian authorities, around that time, were seizing Russian dissenters' computers under the false claim they were pirating Windows software.[426] In 2014, Microsoft

[419] "Putin tells Russia's tech sector: Ditch foreign software or lose out," *CNBC*, (September 9, 2017), https://www.cnbc.com/2017/09/09/putin-tells-russias-tech-sector-ditch-foreign-software-or-lose-out.html.

[420] *Ibid*.

[421] Евгений Лебеденко, « Звезда по имени Linux: почему "военные" ОС прочнее », *old.computerra.ru*, (October 5, 2011), https://old.computerra.ru/vision/609608/.

[422] Alexander Kruglov and Alexey Ramm, « Военные сказали Windows «прощай» », *iz.ru*, (January 9, 2018), https://iz.ru/688478/aleksandr-kruglov-aleksei-ramm/voennye-skazali-windows-proshchai.

[423] Catalin Cimpanu, "Russian military moves closer to replacing Windows with Astra Linux," *ZDNet*, (May 30, 2019), https://www.zdnet.com/article/russian-military-moves-closer-to-replacing-windows-with-astra-linux/; Patrick Tucker, "Russia's Would-Be Windows Replacement Gets a Security Upgrade," *Defense One*, (May 28, 2019), https://www.defenseone.com/technology/2019/05/russias-microsoft-knockoff-gets-security-upgrade/157310/; « Родина в кибербезопасности: российской ОС откроют все секреты », *Izvestia*, (May 24, 2019), https://iz.ru/871218/olga-kolentcova/rodina-v-kiberbezopasnosti-rossiiskoi-os-otkroiut-vse-sekrety.

[424] Alexander Plekhanov, « Почему госструктуры переходят на операционную систему Astra Linux и чем она отличается от Windows », *gol.ru*, (June 26, 2022), https://gol.ru/materials/19205-astra-linux.

[425] David Gewirtz, "Microsoft turns over all Win7 and server source code to Russia's new KGB," *ZDNet*, (July 14, 2010), https://www.zdnet.com/article/microsoft-turns-over-all-win7-and-server-source-code-to-russias-new-kgb/.

[426] Clifford J. Levy, "Russia Uses Microsoft to Suppress Dissent," *The New York Times*, (September 11, 2010), https://www.nytimes.com/2010/09/12/world/europe/12raids.html.

patched vulnerabilities in Windows, Internet Explorer, Microsoft Office, and the .Net Framework.[427] Russian hackers had exploited some of these vulnerabilities.[428]

During this period, Moscow became increasingly paranoid about the Internet as a threat to regime security. It became increasingly concerned about foreign governments use of foreign software and hardware to spy on Russia and otherwise undermine Russia's national security. Astra Linux was an answer to this concern by creating an operating system in which the government had confidence. Today, Mont, Axoft, 1C, Merlion, Elko, and OCS Distribution distribute Astra Linux.[429]

The Astra Linux website does not currently list any distribution partners in the Commonwealth of Independent States (CIS) (Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, and Uzbekistan), but there is a section of the website dedicated to Astra Linux's distributors to those countries.[430] This suggests that the company is looking to market Astra Linux in Russia's "near abroad."[431]

Since invading Ukraine in February 2022, Russia has ramped up its focus on domestic software and Astra Linux. Russia's minister of Digital Development, Communications, and Mass Media stated that the government needed to reduce the barrier for software companies to be included on the state registry, mainly the requirement that companies have more than 50% Russian ownership.[432] In February 2022, according to the Russian paper *Kommersant*, 88.3% of Russian Internet-connected computers used Microsoft Windows.[433] Since then, Microsoft's departure from Russia[434] has catalyzed a Russian government and private-sector push to build and adopt domestic alternatives.

In March, the government tightened the domestic software rules for government organizations. Pursuant to a new presidential decree, all government organizations dealing with "critical information infrastructure" are prohibited from buying foreign software, even if no

---

[427] Sam Frizell, "Microsoft Patches Computer Bug Linked to Russian Hackers," *TIME*, (October 14, 2014), https://time.com/3508067/microsoft-windows-hackers-russia/.

[428] *Ibid*.

[429] « Стать Нашим Партнером », *astralinux.ru*, (accessed November 7, 2022), https://astralinux.ru/partners/.

[430] *Ibid*.

[431] *Ibid*.

[432] "Tech firms request inclusion on Russia's domestic software list – RBC," *Reuters*, (June 8, 2022), https://www.reuters.com/technology/tech-firms-request-inclusion-russias-domestic-software-list-rbc-2022-06-08/.

[433] « «Астра» зовет в экосистему », *Kommersant*, (September 30, 2022), https://www.kommersant.ru/doc/5571844.

[434] Brad Smith, "Microsoft suspends new sales in Russia," *Microsoft.com*, (March 4, 2022), https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/.

domestic replacement exists, beginning on January 1, 2025.[435] This March decree tightened the requirements imposed in the 2016 domestic software decree, which exempted organizations that could not find a foreign software replacement. Then, in October 2022, the Russian government created a marketplace for domestic software as part of the registry.[436]

Developers have also used open-source code to signal their opposition to Putin's war on Ukraine and even to disrupt Russian computer systems. Many open-source software projects had updates following Russia's February invasion that added anti-war, pro-Ukrainian messages into software.[437] At least one project has code added that would wipe a computer if it had a Russian or Belarusian IP address.[438] Sberbank, for example, advised its customers not to update software due to these activities.[439]

Astra Linux usage in Russia has grown in the last year. The Astra Group that makes the software recently opened an office in St. Petersburg and before that had opened offices in Crimea, Ukraine, and in Nizhny Novgorod, Vladivostok, Irkutsk, and Innopolis, Russia.[440] It is currently actively hiring developers, testers, system architects, Linux engineers, information security experts, and other technical personnel.[441] Astra Group has also launched training programs for schoolteachers to learn how to use Astra Linux and to teach it to their students.[442]

Additionally, the Russian government has been purchasing Chinese computers with the prerequisite that Astra Linux comes installed on those systems.[443] This look to China builds on

[435] « Критическая инфраструктура России », *tadviser.ru*, (October 24, 2022), https://www.tadviser.ru/index.php/Статья:Критическая_инфраструктура_России.

[436] "Russian Digital Ministry launches Russian software marketplace," *Interfax*, (October 19, 2022), https://interfax.com/newsroom/top-stories/84064/.

[437] Patrick Howell O'Neill, "Activists are targeting Russians with open-source 'protestware,'" *MIT Technology Review*, (March 21, 2022), https://www.technologyreview.com/2022/03/21/1047489/activists-are-targeting-russians-with-open-source-protestware/.

[438] Steven Vaughan-Nichols, "Corrupted open-source software enters the Russian battlefield," *ZDNet*, (March 21, 2022), https://www.zdnet.com/article/corrupted-open-source-software-enters-the-russian-battlefield/.

[439] O'Neill, "Activists are targeting Russians with open-source."

[440] « ГК «Астра» открыла офис в Санкт-Петербурге », *astralinux.ru*, (November 1, 2022), https://astralinux.ru/news/category-news/2022/gk-astra-otkryila-ofis-v-sankt-peterburge/.

[441] *Ibid*.

[442] « МГОУ и ГК «Астра» запустили программу обучения ос Astra Linux для учителей информатики », *astralinux.ru*, (October 26, 2022), https://astralinux.ru/news/category-news/2022/mgou-i-gk-astra-zapustili-programmu-obucheniya-os-astra-linux/.

[443] « МВД купило тысячи китайских ПК на Astra Linux », *cnews.ru*, (May 16, 2022), https://www.cnews.ru/news/top/2022-05-16_mvd_v_ramkah_gosoboronzakaza.

previous ideas in Russia that China could be a valuable substitute for Western technology.[444] For example, the Chinese telecom Huawei had been playing into the Kremlin's concerns about Western technology and espionage to sell equipment in Russia.[445]

The vision for Astra Linux going forward is not just to have a Russian-produced operating system. Rather, as described by Astra Group's CEO, the goal is to have a full-stack domestic software product for Russian companies, government organizations, and individuals.[446] For example, the company is working on ALD Pro, a system administration tool, and RuPost, a mail server, as part of its software development.[447] It wants to become a global software vendor.[448] Astra Linux currently works with over 4,000 partner software and hardware solutions, some of which can be used in Russian "critical information infrastructure" facilities and the oil and gas industry, and plans to increase that number.[449]

SocialCyber Analysis on Russia

The Margin Research team has developed AI tools to assist with its analysis of Russia's cyber operations. They have enabled a preliminary analysis of personnel who engage in open-source development in China, Russia, North Korea, and Iran in addition to the various institutions and agencies supporting them. By collecting an extensive set of data on the interactions of open-source software contributors, the team has used these tools to identify specific code contributions within the Linux kernel and elsewhere and identify the authors through their email addresses and other identifiers.

An analysis of open-source software and social media has proved its worth in the identification of suspicious cyber activity and potentially malicious cyber operations stemming from Russia and China. The present analytical effort uses novel AI techniques to create an analysis pipeline of Russian cyber operations and the actors involved, localizing suspicious contributors and events for further inspection. Earlier analyses of open-source development lacked the tools

---

[444] Peter Baker, "As Russia Draws Closer to China, U.S. Faces a New Challenge," *The New York Times*, (November 8, 2014), https://www.nytimes.com/2014/11/09/world/vladimir-putin-xi-jinping-form-closer-ties.html.

[445] Justin Sherman, "Huawei's push in Russia exploits Kremlin fears of Western technology," *Atlantic Council*, (November 18, 2020), https://www.atlanticcouncil.org/blogs/new-atlanticist/huaweis-push-in-russia-exploits-kremlin-fears-of-western-technology/; Lauren Dudley, *Part Two: Huawei Enlists Russian Talent and Technology to Ensure Future Innovation*, (New York: Council on Foreign Relations, October 28, 2020), https://www.cfr.org/blog/part-two-huawei-enlists-russian-talent-and-technology-ensure-future-innovation.

[446] « Мы строим глобального вендора системного ПО », *cnews.ru*, (2021), https://www.cnews.ru/projects/2021/astra_linux.

[447] *Ibid*.

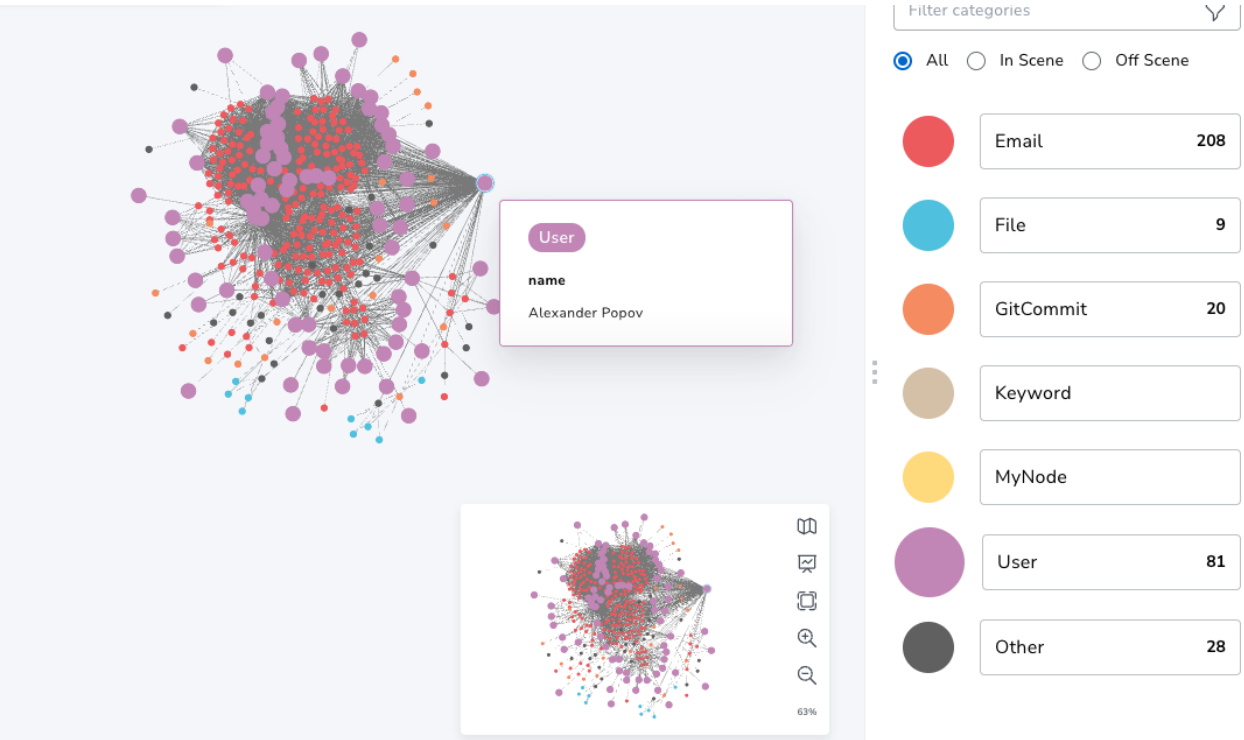
[448] *Ibid*.

[449] « Цифровая надежность », *Kommersant*, (September 20, 2022), https://www.kommersant.ru/doc/5570060.

necessary to uncover suspicious behavior and malicious faith contributions and did not have access to the large body of data collected in the present effort.

The following examples merely scratch the surface of what will be possible with these tools in providing resources for open-source development communities to protect their processes and government, and representatives of user organizations to assess the likelihood that the codebase has been compromised and by whom. They show that data produced by the open-source development process confirm and deepen understanding of the Russian cyber ecosystem that was developed through traditional open-source research methods. The methodology can be applied to other cyber ecosystems, as the research team has already done with respect to China.[450]

Based on the analysis of contributions to the Linux kernel, an individual by the name of Alexander Popov is one of the top Russian contributors. Popov works at Positive Technologies, the U.S.-sanctioned cybersecurity company that defensively and offensively supports the Russian intelligence community. Positive Technologies also runs conferences that the Russian FSB and GRU use to recruit hackers.



[450] See Dave Aitel, et al., *China's Cyber Operations: The Rising Threat to American Security*, *op. cit.*

Alexander Popov studied information security at Moscow State University of Railway Engineering (MIIT) from 2005 to 2011.[451] He is currently a Principal Security Researcher at Positive Technologies (October 2022-present) and before that was a Linux kernel developer and security researcher at Positive (January 2017-October 2022) and a system software engineer at Positive (January 2015-January 2017).[452] Before that, he worked at Telum, a technology company that spun out of the Russian Academy of Sciences' Institute for Information Transmission Problems (a/k/a the Kharkevich Institute)[453] and at Russian Railways, among others.[454] Popov's primary focus at Positive Technologies is Linux kernel vulnerabilities, exploitation techniques, and defensive technologies.[455]

Popov has spoken at a number of cybersecurity conferences since at least 2016, including Positive Technologies' PHDays as well as Nullcon, ZeroNights, Zer0Con, Linux Plumbers Conference, Linux Security Summit North America, OffensiveCon, ISPRS Open Conference, Linux Piter, Open Source Summit Europe, Still Hack Anyway, and LinuxCon Japan. Every one of his talks documented as part of research for this paper focused on the Linux kernel.

One of Popov's recent focus areas is Fuchsia, a Google-developed open-source operating system. Popov has published blogs and given multiple conference talks about debugging the kernel underpinning Fuchsia and then developing exploits for the operating system.[456] Ultimately, he was able to place a rootkit in the operating system.[457]

These novel insights from the SocialCyber project have implications for Russia's domestic technology push and its open-source code and private-sector cybersecurity ecosystem. Not all of Positive Technologies' work appears to be offensive in nature. Based on indications observed, a significant number of security researchers join Positive Technologies to work on defensive cybersecurity projects.

Many of Positive Technologies' advertised solutions focus on cyber defense, including its industrial control system cybersecurity audits, vulnerability management system, financial services cybersecurity offerings, and its industrial cybersecurity suite to help "identify attacks at

---

[451] "Alexander Popov," *ru.linkedin.com*, (accessed October 27, 2022).

[452] *Ibid*.

[453] Russian Academy of Sciences Institute for Information Transmission Problems, "About," *iitp.ru*, (accessed October 27, 2022), http://iitp.ru/en/about; "Cassidian to cooperate with Russian company Telum on public safety communications," *tcca.info*, (February 25, 2013), https://tcca.info/cassidian-to-cooperate-with-russian-company-telum-on-public-safety-communications/.

[454] "Alexander Popov," *ru.linkedin.com*.

[455] "Alexander Popov: Exploiting a Linux Kernel Vulnerability in the V4L2 Subsystem," *OffensiveCon.org*, (February 2020), https://www.offensivecon.org/speakers/2020/alexander-popov.html.

[456] Alexander Popov, "A Kernel Hacker Meets Fuchsia OS," *swarm.ptsecurity.com*, (May 24, 2022), https://swarm.ptsecurity.com/a-kernel-hacker-meets-fuchsia-os/.

[457] *Ibid*.

any stage in an industrial environment and respond to them swiftly."[458] For his part, many of Popov's contributions to the Linux kernel are focused on identifying exploits and patching them.

Positive Technologies is a major Russian government contractor. It makes sense that it would invest time and money in securing open-source projects. Such an effort would be consistent with the Russian government's emphasis on developing domestic technologies in this area. Moscow has accelerated its push for companies to use the Astra Linux operating system instead of foreign offerings like Microsoft Windows. The Russian government should want that system to be as secure as possible because the Ministry of Defense, the FSB Intelligence Service, and other organizations began adopting Astra Linux on computers handling state secrets.

Positive Technologies provides offensive cyber support for the Russian intelligence community. The company is not a monolith; it is probable that different parts of the company perform different functions. The research team estimates that some Positive Technologies employees focus on offensive capabilities while other individuals focus on defensive capabilities. It also may be the case they use their in-house, developed offensive capabilities directly for defensive purposes such as penetration testing.

As the political environment in Russia becomes more repressive, Russian technology companies are even more vulnerable to state control, infiltration, violence, and coercion. The FSB or another Russian security organ is able to exert pressure on Russian developers who might otherwise have nothing to do with offensive capability development for the state. Such pressure could include forcing a developer to include a backdoor in operating system code. Indeed, there is little incentive for the FSB, for example, not to do this, as it is consistent with its normal mode of operation.

These kinds of risks matter for open-source security. The more open-source software is used globally, the more the Russian intelligence community may wish to compromise it for espionage, political, military, or commercial purposes.

Case Study: Positive Technologies' New Bug Bounty Platform

Another component of Russia's open-source ecosystem and hacker community is bug bounties (rewards for discovering and reporting software vulnerabilities/bugs). In the last several months, government officials have spoken publicly about the importance of developing domestic, Russian bug bounty platforms. The effectiveness of these platforms will shape how well Russian companies are able to find and patch vulnerabilities in their systems. The Russian government or its contractors may leverage these platforms to develop exploits, although, for now, the only organizations on the platforms are Russian actors.

At its 2022 PHDays conference, during which it runs cybersecurity code competitions, and provides a podium for presentations and talks on the importance of cybersecurity (including the open-source community and the future of AI for cybersecurity), Positive Technologies launched a

[458] "Solutions," *ptsecurity.com*, (accessed October 27, 2022), https://www.ptsecurity.com/ww-en/solutions/.

bug bounty platform called The Standoff Bug Bounty 365. . The first two companies to join the platform were Positive Technologies itself and Azbuka Vkusa, the Russian supermarket chain.[459]

Russian social media network VK, formerly, VKontakte, otherwise known as "Russia's Facebook" for its similar functionalities and virtually identical interface, joined in August 2022.[460] VK's bug bounty program has more than 40 open projects, with rewards ranging from $100 to $30,000 depending on the vulnerability.[461] As of August 8, 2022, Positive Technologies reported that more than 1,600 researchers have joined the platform and submitted 49 vulnerability reports.[462]

In total, the website lists the following participating companies:

Company Name	Description	Bug Reward	Accepted Reports	Participants in Reports
Pulse (owned by VK)	Personal news recommendation feed	0-180,000 rubles ($0-29,079)	1	2
Boosty (owned by VK)	Author content monetization platform	0-180,000 ($0-29,079)	1	3
DonationAlerts (owned by VK)	Livestreaming donation service	0-600,000 rubles ($0-9,693)	0	1
Tarantool (owned by VK)	Russian database management tool	0-60,000 rubles ($0-969)	0	0
VK People Hub (owned by VK)	Russian employee management tool	0-60,000 rubles ($0-969)	0	2
VK HR Tek (owned by VK)	Russian social network	0-600,000 rubles ($0-9,693)	0	0
VK	Russian social network	0-1,800,000 rubles ($0-29,079)	12	25
Odnoklassniki (owned by VK)	Russian social network	0-600,000 rubles ($0-9,693)	4	11
Mail.ru (owned by VK)	Russian email service	0-1,800,000 rubles ($0-29,079)	11	16
VK Cloud Solutions (owned by VK)	Russian cloud platform	0-900,000 rubles ($0-14,539)	11	9
VK Play (owned by VK)	Russian gaming platform	0-60,000 rubles ($0-969)	3	7
Zen (owned by VK; bought from internet company	Russian news aggregation platform	0-60,000 rubles ($0-969)	0	3

[459] "Russian social network VK joins The Standoff 365 Bug Bounty," *phdays.com*, (August 8, 2022), https://www.phdays.com/en/press/news/russian-social-network-vk-joins-the-standoff-365-bug-bounty/.

[460] *Ibid*.

[461] *Ibid*.

[462] *Ibid*.

Yandex in September 2022)[463]				
TARM (owned by VK)	Russian integrated communications service for the VK Teams, Work Mail, and WorkSpace products	0-155,000 rubles ($0-2,504)	5	7
Uchi.ru (owned by VK)	Russian online education platform	0-60,000 rubles ($0-969)	12	20
Skillbox (owned by VK)	Russian online education platform	0-60,000 rubles ($0-969)	8	16
GeekBrains (owned by VK)	Russian online education platform	0-60,000 rubles ($0-969)	4	8
Algorithmics (owned by VK)	Russian programming platform for children	0-9,000 rubles ($0-145)	5	13
Tetrika (owned by VK)	Russian online education platform teaching school subjects and preparing students for the Unified State Exam (USE) that Russian high school students must pass to attend a university or professional college	0-9,000 rubles ($0-145)	4	10
"Everything else," by VK	VK program for vulnerabilities not captured in the other product focus areas	0-60,000 rubles ($0-969)	7	13
Azbuka Vkusa	Russian supermarket chain	0-100,000 rubles ($0-1,615)	10	35
Positive Technologies	Russian cybersecurity company	0-393,200 rubles ($0-6,352)	4	18
Rambler&Co	Russian media and web services conglomerate	0-100,000 rubles ($0-1,615)	0	10

The companies vary their bug bounty price based on their assessment of the vulnerability's significance. For example, Rambler says that its payments are based on the Common Vulnerability Scoring System (CVSS) version 3.0, but that its internal policies for vulnerabilities set the prices differently.[464] It will pay 100,000 rubles for vulnerabilities ranked critical (scored 9.9-10.0), 35,000-45,000 rubles for vulnerabilities ranked high (8.0-9.8 scoring), 5,000-20,000 rubles for vulnerabilities ranked medium (4.0-7.9), and 2,000 rubles for vulnerabilities ranked low (0.1-3.9 scoring).[465]

[463] Natasha Lomas, "Yandex's sale of News and Zen to VK complete," *TechCrunch*, (September 12, 2022), https://techcrunch.com/2022/09/12/yandex-news-zen-vk-sale-completes/.

[464] "Rambler&Co," *standoff365.com*, (accessed October 6, 2022), https://bugbounty.standoff365.com/en-US/programs/rambler_and_co.

[465] *Ibid*.

Rambler states on the Positive Technologies bug bounty platform that it wants to have submissions focus on remote code execution, injections, and other similar kinds of attacks.[466] It states that it is not interested in, among other things, social engineering vulnerabilities, automatic scan results that do not include proof-of-concept exploits, injecting code into HTPP headers without notable cybersecurity impacts, attacks requiring physical access to target systems, and third-party library vulnerabilities that do not lead to vulnerabilities for the company.[467]

Positive Technologies states on the platform that it bases bug payment on vulnerability type.[468] It pays 90,000-393,200 rubles for remote code execution vulnerabilities; it pays 43,600-224,200 rubles for local files access and manipulation (such as XML external entity injection) vulnerabilities; it pays 36,000-224,200 rubles for injection vulnerabilities (like SQLi injection); it pays 20,000-120,000 rubles for vulnerabilities to bypass administrative authentication; and it pays 45,000-80,000 rubles for server-side request forgery vulnerabilities.[469]

The company will also pay for vulnerabilities discovered in third-party software based on a discretionary pay scale, which is not specified.[470] It states that it will not pay for automated security scan reports, discovery of information about Positive Technologies like IP addresses and DNS records, and reports of, among other things, insecure Secure Socket Layer (SSL)/Transport Layer Security (TLS).[471]

VK states on the platform that it structures its bounty payments according to the following chart.[472] It also states that there are different bug bounty pricing categories for VK ID (the single authorization service for all VK products and services), "Vkcom," in reference to the VK social network itself, and anything else not in those categories:

Vulnerability	VK ID	Vkcom	Anything else
Remote code execution, server-side	1,800,000 rubles ($0-29,079)	1,200,000 rubles	1,200,000 rubles
Remote code execution, mobile app	300,000 rubles	300,000 rubles	300,000 rubles
SQL injection	900,000 rubles	900,000 rubles	900,000 rubles

[466] *Ibid*.

[467] *Ibid*.

[468] "Positive Technologies," *standoff365.com*, (accessed October 6, 2022), https://bugbounty.standoff365.com/en-US/programs/ptsecurity.

[469] *Ibid*.

[470] *Ibid*.

[471] *Ibid*.

[472] « ВКонтакте », *standoff365.com*, (accessed November 14, 2022), https://bugbounty.standoff365.com/programs/vkontakte_vk.

Local file inclusion / remote file inclusion	600,000 rubles	600,000 rubles	600,000 rubles
XML external entity	600,000 rubles	600,000 rubles	600,000 rubles
Server-side request forgery	600,000 rubles	600,000 rubles	600,000 rubles
Server-side request forgery, blind	180,000 rubles	180,000 rubles	180,000 rubles
Insecure direct object reference	60,000 rubles	60,000 rubles	60,000 rubles
Cross-site scripting attack	60,000 rubles	60,000 rubles	60,000 rubles
Open redirect	18,000 rubles	18,000 rubles	18,000 rubles

Positive Technologies expects that, by the end of 2022, 10 to 20 organizations will also join the platform with their own bug bounty programs.[473] It hopes that by 2025 more than 100 other organizations will join.[474] This platform thus may become an important part of vulnerability discovery in Russia and of cultivating Russia's hacker community.

Case Study: Positive Hack Days and the Future of Russia's Open-Source Community

Multiple talks at the 2022 PHDays conference focused on open-source code and open-source community challenges in Russia. They provide a snapshot of how Russian cybersecurity experts and technology developers are thinking about the role of open-source code, development, and security in the broader Russian cyber ecosystem.

In one discussion, Denis Korablev, a Positive Technologies product manager who focuses on open-source code, spoke about what hinders the spread of open-source software in Russia.[475] Korablev said that many Russian enterprises face a psychological hurdle when investing in open-source technology: "when you publish something as a company to public access, there is an illusion that it can be stolen from you." But the real business problem, he said, is when a competitor can use the open-source product to develop a better product and then sell it. He said that publishing open-source code *is not per se* bad for a business.

Korablev added that the current state of geopolitics has changed the landscape for open-source software. "Recent events became geopolitical," he said. "Some countries don't like to use cyber software not from their own countries, not from their own locations." Companies face a challenge because "you are confident in yourself so much, but [buyers] may not believe you. So

[473] "Russian social network VK joins The Standoff 365 Bug Bounty."

[474] *Ibid*.

[475] Denis Korablev and Yuliya Sorokina, "What hinders the spread of open source in Russia?", discussion at Positive Hack Days 2022, (May 18, 2022).

how can you prove it? You can open this code—make it open-source. And this is the only way, the only path, to go to wider geographies in order to make your products popular."

In another discussion, three Positive Technologies employees sat down with a moderator to discuss the issue of import substitution in Russia, that is, in other words, replacing foreign technology with domestic, Russian-made hardware and software.[476] "It's an irreversible process," Aidair Guzairov, one of the individuals, said. "Like it or not, it's going to be done. . . . This is a double Iron Curtain. There are no external technologies, and internally, the customers do not trust foreign products and do not want to buy foreign products." Another speaker, Maxim Filippov, added that even if foreign technology suppliers came back into Russia tomorrow, many domestic companies would not take their products.

Vyacheslav Barkhatov, the third Positive Technologies employee, stated that Russians are increasingly searching for domestic alternatives to foreign technology products. He said that on a website helping Russians to look up domestic software analogues, "in the last, say, 45 days, we had about 9,000 unique hits, unique users, who came to the website to find a Russian analogue to a foreign product." In contrast, *Kommersant* reported in September that Russians' requests to Google to install pirated versions of Microsoft Windows increased 80-250% between the Spring and the Fall.[477]

"Since today, we are fighting a cyber war," Aidair Guzairov said, "these solutions are very much in demand." Frequently, he continued, "once you open the door to a customer, substitute a foreign product there, the vendor can stay there for a long time." Even if the geopolitical reality was different tomorrow, he said, Putin's presidential decree from March already set out goals of replacing foreign software in Russia by 2025. "We don't have much time."

[476] Maxim Filippov, Vyacheslav Barkhatov, Aidair Guzairov, and Vladimir Zapolyansky, "Import substitution," discussion at Positive Hack Days 2022, (May 18, 2022).

[477] « «Астра» зовет в экосистему ».

References

Aitel, Dave, et al., *China's Cyber Operations: The Rising Threat to American Security* (New York: Margin Research, 2022)

Akimenko, Valeriy and Keir Giles, "Russia's Cyber and Information Warfare," *Asia Policy* (2020)

Alazab, Mamoun, "Russia is using an onslaught of cyber attacks to undermine Ukraine's defence capabilities," *The Conversation* (February 24, 2022)

"Alexander Popov: Exploiting a Linux Kernel Vulnerability in the V4L2 Subsystem," *OffensiveCon.org*, (February 2020)

Andrew, Christopher and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West* (London: Penguin Books, 2000)

Angara Security, вошла топ-10 российских поставщиков ИБ-решений », *angarasecurity.ru*, (October 11, 2022)

Annual Threat Assessment of the U.S. Intelligence Community. (Office of the Director of National Intelligence, March 2022)

Appell, James, "The Short Life and Speedy Death of Russia's Silicon Valley," *Foreign Policy*, (May 6, 2015)

APT28: At the Center of the Storm (Milpitas: FireEye, January 2017)

Artificial Intelligence and Autonomy in Russia: Issue 39 (Arlington: Center for Naval Analyses, 2021)

Baker, Peter, "As Russia Draws Closer to China, U.S. Faces a New Challenge," *The New York Times*, (November 8, 2014)

Balmforth, Tom and Maria Tsvetkova, "Russia takes down REvil hacking group at U.S. request – FSB," *Reuters* (January 14, 2022)

Barbashin, Anton, and Alexander Graefand, *Thinking Foreign Policy in Russia: Think Tanks and Grand Narratives* (Washington: Atlantic Council, November 2019)

Bennett, Gordon, *Russia's Foreign Intelligence Service*, (London: UK Conflict Studies Research Center, (March 2000)

Benyumov, Konstantin and Emily Tamkin, "Meet The Woman Who Is Proudly Russia's Troll-In-Chief," *BuzzFeed News*, (October 22, 2018)

Bilyana, Lilly and Joe Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces* (Tallinn: NATO Cooperative Cyber Defense Center of Excellence, 2020)

Blagovest, Yashev, Michael Purcell, and Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU Journal* (Fall 2019)

Blank, Stephen J., "Information Warfare a la Russe," in Phil Williams and Dighton Fiddner (eds.), *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition* (Carlisle: U.S. Army War College Press, 2016)

Blessing, Jason, "Get ready for Russia's cyber retaliation," *The Hill* (March 4, 2022)

Booz-Allen-Hamilton, *Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations* (2020)

Borogan, Irina, and Andrei Soldatov, *The Shadow War: Putin Strips Spies of Ukraine Role*, (Washington: Center for European Policy Analysis, May 9, 2022)

Boston, Scott and Dara Massicot, *The Russian Way of Warfare: A Primer*, (Santa Monica: The RAND Corporation, 2017)

Bowen, Andrew, S., *Russian Cyber Units* (Washington: Congressional Research Service, February 2, 2022)

Bowen, Andrew S., *Russian Military Intelligence: Background and Issues for Congress*, (Washington: Congressional Research Service, November 2021)

Brandt, Jessica and Adriana Pita, *How is Russia conducting cyber and information warfare in Ukraine?* (Brookings: March 3, 2022

Brewster, Thomas, "Wikileaks Release: Hacking Team Says It Sold Spyware To FSB, Russia's Secret Police," *Forbes*, (July 9, 2015)

Brantly, Aaron and Liam Collins, "A Bear of a Problem: Russian Special Forces Perfecting their Cyber Capabilities," *Army Times* (November 28, 2018)

Brumfield, Cynthia, *Russia-linked cyberattacks on Ukraine: A timeline*, (CSO, April 1, 2022)

Cave Brown, Anthony, *Bodyguard of Lies* (New York: Harper & Row, 1975)

Central Intelligence Agency, *Russia, CIA.gov*, (updated August 18, 2022)

Central Intelligence Agency, *The Nature of Soviet Military Doctrine,* SOV 89-10037CX. (April 1989. Declassified April 2000)

Chen, Adrian, "The Agency," *The New York Times*, (June 2, 2015)

Cheravitch, Joe and Lilly Bilyana, *Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond* (Tallinn: NATO Cooperative Cyber Defense Center of Excellence, December 2020)

Chotikul, Diane, *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study* (Monterey: Naval Postgraduate School, July 1986)

Cimpanu, Catalin, "Russian hacker Pavel Sitnikov arrested for sharing malware source code," *The Record,* (May 31, 2021)

Cimpanu, Catalin, "Russian military moves closer to replacing Windows with Astra Linux," *ZDNet*, (May 30, 2019)

Cimpanu, Catalin, "Ukraine discloses identity of Gamaredon members, links it to Russia's FSB," *The Record* (November 4, 2021)

Clapper, James R., Marcel Lettre, and Michael S. Rogers, *Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States* (January 5, 2017)

Connell, Michael and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington: Center for Naval Analyses, March 2017)

Cornish, Paul, *Cyber Security and Politically, Socially, and Religiously Motivated Cyber Attacks* (Strasbourg: European Parliament, February 2009)

Cunningham, Connor, *A Russian Federation Information Warfare Primer* (University of Washington, November 12, 2020)

Cybersecurity and Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure," *CISA.gov*, (February 25, 2016)

Cybersecurity and Infrastructure Security Agency, *Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise*. (May 2021)

Cybersecurity and Infrastructure Security Agency, "Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders," *CISA.gov* (April 26, 2021)

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and National Security Agency, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure* (Revised, March 1, 2022)

Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (2017)

Demberger, Autumn, "Merck Awarded $1.4 Billion for NotPetya After 5 Years of Legal Battle," *Risk & Insurance*, (May 8, 2022)

Dempsey, Judy, "Judy Asks: What Can the West Do About Russia's Bunker Mentality?" *Carnegie Europe*, (July 25, 2012)

Department of Defense Cyber Strategy 2018

Department of Defense, *National Defense Strategy 2022* (March 28, 2022)

Department of Defense. *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*. PP-21-0782. (July 2021)

Department of Health and Human Services. *Major Cyber Organizations of the Russian Intelligence Services* (May 2022)

Department of Homeland Security and Federal Bureau of Investigation, *Joint Analysis Report: GRIZZLY STEPPE – Russian Malicious Cyber Activity* (December 29, 2016)

Department of Homeland Security and Federal Bureau of Investigation, *Joint Analysis Report: Enhanced Analysis of GRIZZLY STEPPE – Russian Malicious Cyber Activity* (February 10, 2017)

Department of Homeland Security, CISA, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure* (April 30, 2022)

Department of Justice, "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide," *Justice.gov* (March 24, 2022)

Department of Justice, "Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," *Justice.gov*, (October 19, 2020)

Department of Justice, "Russian National Receives 18 Month Prison Sentence for Smuggling High-Tech Night Vision Technology to Russia," *Justice.gov* (October 9, 2014)

Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," *Justice.gov* (October 19, 2020)

Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," *Justice.gov* (March 15, 2017)

Department of the Treasury, "Russia-related Designations and Designation Update; Issuance of Russia-related General Licenses," *treasury.gov*, (April 20, 2022)

Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," *Treasury.gov*, (April 15, 2021)

Department of the Treasury, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware," *Treasury.gov* (December 5, 2019)

Department of the Treasury, "Treasury Sanctions Russian Officials in Response to the Novichok Poisoning of Aleksey Navalny," *Treasury.gov* (March 2, 2021)

Department of the Treasury, "Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors," *Treasury.gov* (March 3, 2022)

Department of the Treasury, "Treasury Sanctions Russian Federal Security Service Enablers," *Treasury.gov*, (June 11, 2018)

Department of the Treasury, "Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," *Treasury.gov* (March 31, 2022)

Diebert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgian War," *Security Dialogue* (February 2012)

Dobbins, James, Howard J. Shatz, and Ali Wyne, *Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue: Different Challenges, Different Responses* (Santa Monica: The RAND Corporation, 2019)

Dudley, Lauren, *Part Two: Huawei Enlists Russian Talent and Technology to Ensure Future Innovation*, (New York: Council on Foreign Relations, October 28, 2020)

Eckel, Mike, "In Moscow Treason Trial, A Major Scandal For Russian Security Agency," (RadioFreeEurope/RadioLiberty, February 27, 2019)

Eckhardt, Ivan, "Jurisdictional Risk: The Czech Republic," *DowJones.com*, (May 2020)

Electronic Frontier Foundation, "US v. ElcomSoft Sklyarov," *eff.org*, (accessed October 3, 2022)

Estonian Foreign Intelligence Service, *International Security and Estonia 2018*

Farivar, Cyrus, "Hacking Team apparently violated EU rules in sale of spyware to Russian agency," *Ars Technica*, (July 17, 2015)

Fendorf, Kyle and Jessie Miller, *Tracking Cyber Operations and Actors in the Russia-Ukraine War,* (New York: Council on Foreign Relations, March 24, 2022)

Finch, Ray C., "Ensuring the Political Loyalty of the Russian Soldier," *Military Review* (July-August 2020)

Fox-Brewster, Tom, "'State sponsored' Russian hacker group linked to cyber attacks on neighbors," *The Guardian*, (October 29, 2014)

Foy, Henry, "Russian IT firm IBS freezes planned IPO amid sanctions uncertainty," *Financial Times*, (April 13, 2018)

Franke, Ulrik, *War by Non-Military Means: Understanding Russian Information Warfare*.. (Stockholm: Swedish Defense Research Agency, March 2015)

Frizell, Sam, "Microsoft Patches Computer Bug Linked to Russian Hackers," *TIME,* (October 14, 2014)

"Грузить по полной программе," *Meduza* (September 3, 2015)

Galeotti, Mark, *Active Measures: Russia's Covert Geopolitical Operations* (Garmisch-Partenkirchen: European Center for Security Studies, June 2019)

Galeotti, Mark, "GRU (GU) facing a little purge? If so, it's not spy less, but spy better," *In Moscow's Shadows* (October 9, 2018)

Galeotti, Mark, "Active Measures: Russia's Covert Global Reach," in Graeme P. Herd, *Russia's Global Reach: A Security and Statecraft Assessment* (Garmisch-Partenkirchen: Marshall Center, 2021)

Galeotti, Mark, *Putin's Hydra: Inside Russia's Intelligence Services* (Berlin: European Council on Foreign Relations, May 2016)

Galeotti, Mark, "Russia's Murderous Adhocracy," *The Moscow Times*, (August 22, 2020)

Gatlan, Sergiu, "White House pins Ukraine DDoS attacks on Russian GRU hackers," *Bleeping Computer*, (February 18, 2022)

Gewirtz, David, "Microsoft turns over all Win7 and server source code to Russia's new KGB," *ZDNet*, (July 14, 2010)

Giles, Keir, *Assessing Russia's Reorganized and Rearmed Military* (Washington: Carnegie Endowment for International Peace, May 2017)

Giles, Keir *Handbook of Russian Information Warfare* (Rome: NATO Defense College, November 2016)

Giles, Keir and Anthony Seaboyer, "The Russian Information Warfare Construct," *Defense Research and Development Canada* (October 2019)

Goodin, Dan, "US and allies say Russia waged cyberattack took out satellite network, *Ars Technica* (May 10, 2022)

Government of the Russian Federation, "Maksut Shadayev," *government.ru,* (accessed October 14, 2022)

Graham, Loren, "Science in the New Russia," *Issues* (Summer 2003)

Graham, Thomas, "The Sources of Russia's Insecurity," *Survival,* (2010)

Greenberg, Andy, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019)

Greenberg, Andy, "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction," *WIRED,* (September 12, 2019)

Greenberg, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED,* (August 22, 2018)

Greenberg, Andy, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," *WIRED,* (October 17, 2019)

Grzegorzewski, Mark and Christopher Marsh, *Incorporating the Cyberspace Domain: How Russia and China Exploit Asymmetric Advantages in Great Power Competition,* (West Point: Modern War Institute, March 15, 2021)

Gurganus, Julia and Eugene Rumer, *Russia's Global Ambitions in Global Perspective* (Washington: Carnegie Endowment for International Peace, February 2019)

Guzairov, Aydar, "The task of sovereign internet can be solved no earlier than in two years in Russia," *Realnoe Vremya,* (March 17, 2021)

Hakala, Janne and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace* (Riga: NATO Strategic Communications Center of Excellence, June 2021)

Halpern, Sue, "The Drums of Cyberwar" (review of Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, 2019, 348 pp.), *The New York Review of Books*, vol. LXVI, no. 20 (19 December 2019)

Haskins, Caroline, "Intel, SpaceX, Philip Morris, and dozens of other US companies were in a leaked database of users for a Russian facial recognition company," *Business Insider,* (July 30, 2022)

Henderson, Peter, "Russian president downloads Silicon Valley success," *Reuters,* (June 23, 2010)

Her Majesty's Treasury, Office of Financial Sanctions Implementation. *Financial Sanctions Notice: Russia,* (London: Office of Financial Sanctions Implementation, April 2022)

Hill, Fiona and Clifford G. Gaddy, *What makes Putin tick, and what the West should do*, (Washington: Brookings Institution, January 13, 2017)

"How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine," *Bellingcat,* (April 26, 2021)

"How the Dutch foiled Russian 'cyber-attack' on OPCW," *BBC,* (October 4, 2018)

"Investigative Report: On The Trail Of The 12 Indicted Russian Intelligence Officers," RadioFreeEurope/RadioLiberty (July 19, 2018)

Ivakhnyuk, Irina, *Brain Drain from Russia: in Search for a Solution* (Warsaw: Centre for International Relations, 2006)

Jankowski, Dominik P., *Russia and the Technological Race in an Era of Great Power Competition* (Washington: Center for Strategic & International Studies, September 2021)

Jasper, Scott, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington: Georgetown University Press, 2020)

Kissinger, Henry, *Conversation with Mikhail Gorbachev*, January 17, 1989, trans. Svetlana Savranskaya, Notes of A. S. Chernyaev, Archive of the Gorbachev Foundation, Cold War International History Project

Korobkov, Andrei V. and Zhanna A. Zaionchkovskaia, "Russian brain drain: Myths v. reality," *Communist and Post-Communist Studies*, (September/December 2012)

Kowalska, Marta, *Analysis of the Russian 'Strategy for the Development of an Information Society,'* (Warsaw: Center for Propaganda and Disinformation Analysis, May 25, 2017)

Kozlov, Vladimir, "Russian Tech Industry Faces Coronavirus Brain Drain," *The Moscow Times*, June 17, 2020,

Kramer, Andrew E., "How Russia Recruited Elite Hackers for Its Cyberwar," *The New York Times*, (December 29, 2016),

Krebs, Brian, "Russia to Rent Tech-Savvy Prisoners to Corporate IT?" *Krebs On Security*, (May 2, 2022)

Kruglov, Alexander and Alexey Ramm, « Военные сказали Windows «прощай» », *iz.ru*, (January 9, 2018)

Krutov, Mark and Sergey Dobrynin, « Зять на 5 миллионов », *Svoboda* (December 9, 2019)

Kux, Dennis, "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters* (1985)

Levy, Clifford J., "Russia Uses Microsoft to Suppress Dissent," *The New York Times*, (September 11, 2010),

Lewis, James A., *Cyber War and Ukraine* (Washington: Center for Strategic and International Studies, June 2022)

Lysenko, Volodymyr and Catherine Brooks, "Russian information troops, disinformation, and democracy," *First Monday,* (May 2018)

Nakashima, Ellen and Alex Horton, "Russian government hackers have likely penetrated critical Ukrainian computer systems, U.S. says," *Washington Post* (February 15, 2022)

National Security Archive, *Cyber Brief: GRU Cyber Operations* (July 18, 2018)

McWhirt, Matthew, Daniel Smith, Omar Toor, and Brian Turner, "Proactive Preparation and Hardening to Protect Against Destructive Attacks," *Mandiant.com*, (January 14, 2022)

Madnick, Stuart, "What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare," *Harvard Business Review* (March 7, 2022)

Mardiste, David, "Russia to Estonia: Don't move our statue," *Reuters*, (January 25, 2007)

Markoff, John, "Before the Gunfire, Cyberattacks," *The New York Times* (August 12, 2008)

Marks, Joseph, "Is Russia or China the biggest cyber threat? Experts are split," *The Washington Post*, (January 20, 2022)

Mattis, Peter, "Contrasting China's and Russia's Influence Operations," *War on the Rocks,* (January 16, 2018)

MacFarquhar, Neil, "Inside the Russian Troll Factory: Zombies and a Breakneck Pace," *The New York Times,* (February 18, 2018)

Medvedev, Sergei A.,. *Offense-Defense Theory Analysis of Russian Cyber Capability*. (Monterey: U.S. Naval Postgraduate School, March 2015)

"Moscow's cyber defense," *Meduza,* (July 19, 2017)

Minibaev, Eugene, « Предметно-ориентированный отладчик для системы динамической двоичной трансляции QEMU », *Research Gate,* (April 2019)

Moody, R. Adam, "Reexamining Brain Drain from the Former Soviet Union," *The Nonproliferation Review* (Spring/Summer 1996)

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)

Myers, Steven Lee, "Russia Rebukes Estonia for Moving Soviet Statue," *The New York Times,* (April 27, 2007)

Nocetti, Julien, "Russia's 'dictatorship-of-the-law' approach to internet policy," *Internet Policy Review* (November 2015)

O'Neill, Patrick Howell, "Activists are targeting Russians with open-source 'protestware,'" *MIT Technology Review,* (March 21, 2022)

O'Neill, Patrick Howell, "Russia hacked an American satellite company one hour before the Ukraine invasion, *MIT Technology Review* (May 10, 2022)

O'Neill, Patrick Howell, "The internet runs on free open-source software. Who pays to fix it?" *MIT Technology Review*, (December 17, 2021)

Osborn, Andrew, "Russian spy service punishes trainee agents for showy public celebration," *Reuters,* (July 14, 2016)

Page, Carly, "Russia's FSB 'shuts down' notorious REvil ransomware gang," *TechCrunch,* (January 14, 2022)

Pieper, Moritz, "*Russkiy Mir:* The Geopolitics of Russian Compatriots Abroad," *Geopolitics* (2020)

Plekhanov, Alexander, « Почему госструктуры переходят на операционную систему Astra Linux и чем она отличается от Windows », *gol.ru*, (June 26, 2022)

Pomerleau, Mark, "Russia and China devote more cyber forces to offensive operations than US, says new report," *C4ISRNET*, (February 14, 2022)

Popov, Alexander, "A Kernel Hacker Meets Fuchsia OS," *swarm.ptsecurity.com,* (May 24, 2022)

Possehl, Suzanne, "Russian Brain Drain Flows Directly Into U.S. Science Talent Reservoir," *Los Angeles Times*, (February 26, 1995)

Poulsen, Kevin, "This Hacker Party Is Ground Zero for Russia's Cyberspies," *The Daily Beast,* (August 4, 2018)

President of Russia, "Presidential Executive Office subdivisions," *Kremlin.ru,* (last accessed August 1, 2022)

Prothero, Mitch, "A secret Russian assassination squad has proved 'they can get to anyone' in Europe, but there's one problem. They're really sloppy," *Business Insider,* (October 9, 2019)

"Putin abolishes Rospechat, Rossvyaz, assigns their duties to Ministry of Digital Development, Communications and Mass Media," *Interfax,* (November 20, 2020)

"Putin tells Russia's tech sector: Ditch foreign software or lose out," *CNBC,* (September 9, 2017)

Putin, Vladimir, *On the Historical Unity of Russians and Ukrainians* (July 12, 2021)

Pynnöniemi, Katri and Martti J. Kari, *Russia's New Information Security Doctrine: Guarding a besieged cyber fortress* (Helsinki: Finnish Institute of International Affairs, December 2016)

Rapid7, "The Top 5 Russian Cyber Threat Actors to Watch," *Rapid7.com* (March 3, 2022)

Respekt, "Czech intelligence uncovered Russian hackers using IT company front," *Radio Prague International* (March 18, 2019)

Reevell, Patrick, "Inside one of the largest hacking conferences in Russia," *ABC News,* (May 17, 2018)

Reynolds, Maura, "'Yes, He Would': Fiona Hill on Putin and Nukes," *Politico* (February 28, 2022)

Rice, Dakota Salavat and Karl Bahm, *The Nature of Russian and Soviet Intelligence Agencies,* (Superior: University of Wisconsin, 2018),

Rid, Thomas, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020)

Roblin, Sebatian, "Why does Russia Turn to These Sloppy Assassins to Do the Dirty Work?" *The National Interest* (August 27, 2021)

Rostow, Nicholas, "Consequences," *Naval War College Review,* (Autumn 2014)

Roth, Andrew, "String of own goals by Russian spies exposes a strange sloppiness," *The Guardian* (October 5, 2018)

"Russia Expands Restrictions on Government Procurement of Foreign Software and Hardware," *jonesday.com,* (September 2016)

Russia Military Power: Building a Military to Support Great Power Aspirations. DIA-11-1704-161. (Defense Intelligence Agency, 2017)

"Russian Digital Ministry launches Russian software marketplace," *Interfax,* (October 19, 2022)

"Russian Federation: Banned purchase of foreign software in state and municipal orders," *Global Trade Alert,* (November 16, 2015)

Russian Federation. Об утверждении Концепции гуманитарной политики Российской Федерации за рубежом (Concept of the Humanitarian Policy of the Russian Federation Abroad, September 5, 2022)

Russian Government, *Information Security Doctrine of the Russian Federation* (September 9, 2000)

"Russian social network VK joins The Standoff 365 Bug Bounty," *phdays.com*, (August 8, 2022)

"Russia's Wagner Group opens defence tech centre in St Petersburg," *The Guardian* (November 4, 2022)

Sabala, Joe, "Intercepted Call Reveals Russian Frustration Over Defective Equipment," *The Defense Post* (June 20, 2022).

Salt, Alexander and Maya Sobchuk, *Russian Cyber-Operations in Ukraine and the Implications for NATO* (Calgary: Canadian Global Affairs Institute, August 2021)

Sarts, Janis, *Prepared Statement of Janis Sarts, Director of NATO Strategic Communications Centre of Excellence on Russian Interference in European Elections, United States Senate Select Committee on Intelligence* (June 28, 2017)

Schmitt, Michael N., "Russian Cyber Operations and Ukraine: The Legal Framework," *Articles of War* (Westpoint, January 16, 2022)

Schoen, Fletcher and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, (Washington: National Defense University Press, 2012)

Sedkowski, Wiktor, *Welcome to Cyberwar* (Warsaw Institute, December 12, 2017)

Segal, Adam, "Peering Into the Future of Sino-Russian Cyber Security Cooperation," *War on the Rocks*, (August 10, 2020)

Seibt, Sébastian, "Unit 29155, the Russian spies specializing in 'sabotage and assassinations,'" *France24* (April 20, 2021)

Shalkovskyi, Volodymyr, *An Analysis of the Brain Drain Phenomenon in the Field of Development of Chemical and Biological Weapons in Russia During the 1990s* (Monterey: U.S. Naval Postgraduate School, June 2002)

Sherman, Justin, "Digital Active Measures: Historical Roots of Contemporary Russian Cyber and Information Operations," *Georgetown Security Studies Review* (April 2, 2022)

Sherman, Justin, "Huawei's push in Russia exploits Kremlin fears of Western technology," *Atlantic Council*, (November 18, 2020)

Sherman, Justin, *Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior* (Washington: Atlantic Council, July 2021)

Sherman, Justin, *Russia's War for Control of Global Internet Governance* (Social Science Research Network, May 2022)

Smith, Brad, "Microsoft suspends new sales in Russia," *Microsoft.com*, (March 4, 2022),

Smith, R. Jeffry, "Gates Fear Soviet 'Brain Drain,'" *The Washington Post*, (January 16, 1992)

Socor, Vladimir, "Putin Inflates 'Russian World' Identity, Claims Protection Rights," *Eurasia Daily Monitor* (July 2014)

Soldatov, Andrei and Michael Weiss, "Inside Russia's Secret Propaganda Unit," *Newsline Magazine*, (December 7, 2020)

Soldatov, Andrei and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: Public Affairs, 2015)

Soshnikov Andrey and Svetlana Reuters, « Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ », *BBC Russia*, (July 19, 2019)

Sosnitsky,, Vladimir, « ЭРА пополняется новобранцами из Тулы, » *Krasnaya Zvezda*, (August 5, 2019)

Special Counsel Robert S. Mueller, III, *Report on the Investigation into Russian Election Interference in the 2016 Presidential Election: Submitted to the Attorney General Pursuant to 28 CFR §600.8(c)* (March 2019)

Stronski, Paul and Nicole Ng, *Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic* (Washington: Carnegie Endowment for International Peace, February 2018)

Stedman, Scott, "Russian Cybersecurity Firm Draws U.S. Federal Scrutiny, Concern from National Security Experts," *Forensic News*, (January 20, 2022)

Stone, Jeff, "Rare cybercrime enforcement in Russia yields 25 arrests, shutters 'BuyBest' marketplace," *CyberScoop*, (March 25, 2020)

"Strategy for Information Society Development until 2030 approved," *kremlin.ru*, (May 10, 2017)

Subbotin, Alexander and Samin Aref, "Brain drain and brain gain in Russia: Analyzing international migration of researchers by discipline using Scopus bibliometric data 1996-2020," *Scientometrics* (2021)

Sukhankin, Sergey, "Russia Beefs up Its Offensive Cyber Capabilities," *Eurasia Daily Monitor* (November 2016)

Suslov, Mikhail, "'Russian World' Concept: Post-Soviet Geopolitical Ideology and the Logic of 'Spheres of Influence,'" *Geopolitics* (2018)

Tapon, Frances, "The Bronze Soldier Explains Why Estonia Prepares For A Russian Cyberattack," *Forbes*, (July 7, 2018)

Tashev, Blagovest, Michael Purcell, and Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU Journal* (Fall 2019)

"Tech firms request inclusion on Russia's domestic software list – RBC," *Reuters*, (June 8, 2022)

"The FSB's personal hackers," *Meduza*, December 12, 2019

"The Top 5 Russian Cyber Threat Actors to Watch," *Rapid7.com*, (March 3, 2022)

The Military Doctrine of the Russian Federation (April 22, 2000)

The White House, *Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh* (February 18, 2022)

Thomas, Timothy L., *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice* (Fort Leavenworth: Foreign Military Studies Office, October 2000)

Thomas, Timothy, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* (2004)

Thomas, Timothy L., *Russian and Chinese Information Warfare: Theory and Practice* (Fort Leavenworth: Foreign Military Studies Office, June 2004)

Thomas, Timothy L., "Russian Information Warfare Theory: The Consequences of August 2008," in Stephen J. Blank and Richard Weitz (eds) *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* (Carlisle: U.S. Army War College Press, 2010)

Toianovski Antonin and Ellen Nakashima, "How Russia's military intelligence agency became the covert muscle in Putin's duels with the West," *The Washington Post*, (December 28, 2018)

Torsti, Pilvi, "Why do History Politics Matter?: The Case of the Estonian Bronze Soldier," *University of Helsinki,* (2008)

Traynor, Ian, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian,* (May 16, 2007)

Tucker, Patrick, "Russia's Would-Be Windows Replacement Gets a Security Upgrade," *Defense One*, (May 28, 2019)

"Two Russian intelligence front companies uncovered in Czech Republic," *uawire.org,* (March 20, 2019)

United Kingdom Foreign, Commonwealth, & Development Office, "Russia's FSB malign activity: factsheet," *gov.uk,* (April 5, 2022)

United States v. Akulov, et al., (21-cr-20047) (D.C. KS., 2021)

United States v. Andrienko, et al. (20-cr-316)(USDC, WDPA, October 2020)

United States v. Dokuchaev (17-cr-103)(USDC, NDCA, February 2017)

United States v. Elcomsoft (01-cr-20138)(USDC, NDCA, May 2, 2002)

United States v. Fishenko (12-cr-626) (E.D.N.Y. July 29, 2013)

United States v. Gladkikh, (21-cr-442) (D.C. DC, 2021)

United States v. Ionov, (22-cr-259) (M.D. FL, July 26, 2022)

United States v. Morenets, (18-cr-263) (DC WDPA., 2018)

United States v. Netyksho, et al (18-cr-00215) (D.C. DC, July 13, 2018)

United States v. Yakubets, (19-cr-342) (D.C., WD PA, 2019)

"US media should apologize for two years of anti-Russian propaganda — Foreign Ministry," *TASS,* (March 26, 2019)

"'V' for 'Vympel'"; "FSB's Magnificent Seven: New Links between Berlin and Istanbul Assassinations," *Bellingcat* (June 29, 2020)

"'V' for 'Vympel': FSB's Secretive Department 'V' Behind Assassination Of Georgian Asylum Seeker in Germany," *Bellingcat* (February 17, 2020)

Vaughan-Nichols, Steven, "Corrupted open-source software enters the Russian battlefield," *ZDNet*, (March 21, 2022),

Vendil, Pallin, Carolina and Susanne Oxenstierna. *Russian Think Tanks and Soft Power*. (Stockholm: Swedish Defense Research Agency, August 2017)

Vilmer, Jean-Baptiste Jeangène and Paul Charon, "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare," *War on the Rocks*, (January 21, 2020)

Vorobyov, Niko, "'Criminal adventure': Ukraine war fuels Russia's brain drain," *Al Jazeera*, (May 23, 2022),

Wagner, Abraham and Nicholas Rostow, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2020).

Wagner, Abraham R., *Henry Kissinger: Pragmatic Statesman in Hostile Times* (New York: Routledge, 2020).

Walton, Calder, "What's Old is New Again: Cold war Lessons for Countering Disinformation, *Texas National Security Review* (Fall 2022).

Weinberger, Sharon, "Hacked Emails Reveal Russian Plans to Obtain Sensitive Western Tech," *The Intercept*, (May 28, 2015)

"What is Petya and NotPetya Ransomware?" *Trellix*, (accessed September 6, 2022)

White House, "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government," *WhiteHouse.gov*, (April 15, 2021)

Wilde, Gavin, "In Russia's Information War, a New Field of Study Gains Traction," *New Lines Magazine* (September 14, 2022)

Yasmann, Victor, "Russia: Monument Dispute With Estonia Gets Dirty," *Radio Free Europe/Radio Liberty*, (May 4, 2007)

"Your name is on some FSB officer's list," *Meduza*, (May 19, 2021)

Zabierek, Lauren, "Wide range of possible targets for Russian cyber strikes, from infrastructure to smartphones," *The Harvard Gazette* (February 24, 2022)

Zdanevich, Andrei, "Why do Russians officials still prefer to use Microsoft?" *Russia Beyond*, (August 9, 2016)

Zetter, Kim, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, (March 3, 2016)

Zevelev, Igor, *The Russian World in Moscow's Strategy* (Washington: Center for Strategic & International Studies, August 22, 2016)

Zysk, Katarzyna, "Defense innovation and the 4th industrial revolution in Russia," *Journal of Strategic Studies*, (2021)

List of Abbreviations

AI—Artificial Intelligence

APT—Advanced Persistent Threats

BIS—Czech Security Information Service (acronym shared with U.S. Department of Commerce's Bureau of Industry and Security)

CAR—Central African Republic

CIA—Central Intelligence Agency (U.S.)

CIS—Commonwealth of Independent States

CISA—Cybersecurity and Infrastructure Protection Agency (U.S.)

CTF—Capture the Flag (competition)

DDoS—Distributed Denial of Service

DMCA—Digital Millennium Copyright Act

FIRST—Forum of Incident Response and Security Teams

FSB—Russian Federal Security Service

GRITs—GRU's 72nd Main Intelligence Information Center

GRU—Russian Military Intelligence Agency

GRU GTsSS—Russian GRU Main Special Service Center

GRU GTsST—Russian GRU Main Center for Special Technologies

IARPA—Intelligence Advanced Research Projects Agency (U.S.)

ICANN—International Corporation for Assigned Names and Numbers

ICRC—International Committee of the Red Cross

IP—Internet Protocol

ISP—Internet Service Provider

IT— Information Technology (-ies)

KGB—Soviet Committee for State Security

MIPT—Moscow Institute of Physics and Technology

MIREAv—Russian Technological University

NIST—National Institute of Standards and Technology (U.S.)

NSA—National Security Agency (U.S.)

PMC—Private Military Company

RSB—Russian Security Service (full name: RSB Group; the private military company)

SDK—Software Development Kit

SVR—Russian Foreign Intelligence Service