Russian Cyberwarfare:

Unpacking the Kremlin's Capabilities

Andrei Soldatov and Irina Borogan

ABOUT CEPA

The Center for European Policy Analysis (CEPA)'s mission is to ensure a strong and enduring transatlantic alliance rooted in democratic values and principles with strategic vision, foresight, and policy impact. Through cutting-edge research, analysis, and programs we provide fresh insight on energy, security, and defense to government officials and agencies; we help transatlantic businesses navigate changing strategic landscapes; and we build networks of future Atlanticist leaders.

Cover photo credit: A man looks on a screen showing polling stations, at the headquarters of Russia's Central Election Commission in Moscow, Russia September 19, 2021. REUTERS/Shamil Zhumatov/Alamy Stock Photo

Contents

About the Authors

Andrei Soldatov is a nonresident senior fellow with the Center for European Policy Analysis (CEPA). Andrei is a Russian investigative journalist, co-founder, and editor of Agentura.ru, a watchdog of the Russian secret services' activities. He has covered security services and terrorism issues since 1999. In October 2012, Agentura.Ru, Privacy International, and Citizen Lab launched the joint project 'Russia's Surveillance State' with Andrei Soldatov as a head of the project, to undertake research and investigation into surveillance practices in Russia, including the trade in and use of surveillance technologies. The project's research over surveillance measures introduced by the Russian authorities at the 2014 Winter Olympics was run by the Guardian as a frontpage story. He is co-author with Irina Borogan of *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (PublicAffairs, 2010), *The Red Web: The Kremlin's War on the Internet* (PublicAffairs, 2015), and *The Compatriots: The Brutal and Chaotic History of Russia's Exiles, Émigrés, and Agents Abroad* (PublicAffairs, 2019).

Irina Borogan is a nonresident senior fellow with the Center for European Policy Analysis (CEPA). Irina is a Russian investigative journalist, co-founder, and deputy editor of Agentura.ru, a watchdog of the Russian secret services' activities. Borogan reported on terrorist attacks in Russia, including hostage takings in Moscow and Beslan. In 1999 Borogan covered the NATO bombing in Yugoslavia, and in 2006 she covered the Lebanon War and tensions in the West Bank and Gaza Strip. She also chronicled the Kremlin's campaign to gain control of civil society and strengthen the government's police services under the pretext of fighting extremism. She is co-author with Andrei Soldatov of *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (PublicAffairs, 2010), The Red Web: *The Kremlin's Wars on the Internet* (PublicAffairs, 2015) and *The Compatriots: The Brutal and Chaotic History of Russia's Exiles, Émigrés, and Agents Abroad* (PublicAffairs, 2019).

Acknowledgments

This report – *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities* – is part of CEPA's ongoing work on Russia's cyber operations and below-threshold threats. The authors extend their gratitude to the reviewers who provided insight and feedback on earlier drafts of this report. In particular, we thank for their invaluable comments and suggestions Sam Greene, Director for Democratic Resilience at CEPA; Jason Israel, Senior Fellow at CEPA; and Gavin Wilde, Senior Fellow at the Carnegie Endowment for International Peace. We are also grateful for the insights and contributions from the experts who attended CEPA's roundtables in June and July and the research support from CEPA's Research Assistant, Guga Chomakhidze. Finally, a special thank you to the entire CEPA team for their support and guidance on this report.

This publication was funded by the Russia Strategic Initiative, US European Command, Stuttgart, Germany. Opinions, arguments, viewpoints, and conclusions expressed in this work do not represent those of RSI, US EUCOM, the Department of Defense, or the US Government. This publication is cleared for public release.

1. Overview

In the unsettling landscape of Russia's ongoing war in Ukraine, cyber remains one of the most enduring mysteries.

Even before Russian troops invaded Ukraine in February, many experts in the West, in Ukraine, and in Russia believed Moscow would use cyberattacks to inflict major damage on Ukraine prior to or after the start of the military offensive. Indeed, Russia has extensive and formidable cyber capabilities. Reality, however, has played out differently.

Exactly why cyber has not been a consequential front in Russia's invasion of Ukraine is unknown. It may be that Ukrainian cyberspace proved to be much better protected than some thought. Or it may be that Russia did not use its offensive cyber capabilities because the Kremlin interfered in every aspect of the preparation of the war, from military planning to cyber activities. The Kremlin wanted the invasion to play out as a "special operation" (in the Kremlin's words), not a conventional military offensive. In this, as in much else, the Kremlin greatly miscalculated.

While an answer to the mystery of Russian cyber successes and failures in and around Ukraine is beyond the scope of this report, the case is nonetheless instructive, underlining the importance of understanding how Russian cyber operations are governed. The political element has always been decisive in the Russian cyber playbook, much more so than in other parts of the Russian security state. It, thus, comes as no surprise that over the years the command-and-control structure managing Russian cyber operations has developed into something very different.

The list of Russian cyber actors is long and complicated. It includes private entities, both legitimate and criminal, alongside traditional security services, the military, and the top political level where decisions are made. The relationship among these actors has changed quite significantly in the past six years. This report is an attempt to map the Russian cyber landscape and to help understand the intricate web of cyber actors.

Key Russian cyber actors include:

- The FSB: The Federal Security Service (Federalnaya Sluzhba Bezopasnosti; FSB) is a major domestic security and intelligence agency. In cyber, the FSB's capabilities are divided between those the agency has been building since the late 1990s (the 18th Center, or Information Security Center) and the capabilities the FSB acquired in 2003 when it absorbed several departments of the Russian electronic intelligence (ELINT) agency, the Federal Agency for Government

Communications and Information, or FAPSI (the 16th Center of the FSB or the Center of Electronic Intelligence in Communications).

- The SVR: The Foreign Intelligence Service (Sluzhba Vneshney Razvedki; SVR) is Russia's spy agency, a direct successor to the foreign intelligence branch of the KGB. The agency never went through any structural reforms, but its capabilities were significantly expanded in the 2010s, including in cyber.
- The military: The cyber capabilities in Russia's military are run by two directorates within Russia's General Staff: the GU (or the Main Intelligence Directorate; GRU) and the 8th Directorate. These two directorates run operations and supervise Russian cyber troops and the military research and development effort. Cyber command was never launched despite several attempts in the early 2010s.
- The Presidential Administration: The direct successor to the Central Committee of the Communist Party, the Presidential Administration supervises Russia's intelligence and security services. An integral part of the administration is Russia's Security Council, which provides strategic thinking in all areas of national security, including cyber; it is also a government body tasked with maintaining contact with its Western counterparts, including a cyber "red line" between Moscow and Washington.
- Private cybersecurity companies: These companies are tied into Russia's cyber effort via networks of official and unofficial contacts. Their role is to provide expertise and help with recruitment efforts.

Despite this broad range of actors involved in cyber operations on various fronts, Russia doesn't have a unified cyber command. Rather, coordination with the political decision-makers is done at the Presidential Administration level, with Russia's Security Council an integral part of the process. Moreover, unlike in the conventional field of operations, there is no strict division of labor between the agencies in the cyber domain. Agencies traditionally focused on foreign targets have attacked domestic targets (including nongovernmental organizations, journalists, and the Russian opposition). Outside Russia, the military has targeted political and private industry and the SVR and FSB have attacked military targets, and vice versa.

While reliable data are limited, this report delves deeply into the history and evolution of Russia's cyber actors, revealing a remarkably fluid and informal landscape, which is often difficult to interpret and navigate even for those who operate within it. What emerges is a system of cyber operations that is:

1. Coordinated through a set of political processes centered on the Presidential Administration and the Security Council, rather than a traditional, military-style command structure;

2. Characterized by significant overlap in mission and capability, often leading to competition for resources and sometimes to problems of coordination and conflict;
3. Subject to a significant degree of informality and political maneuvering, as different actors report to the Presidential Administration and Security Council via different channels and with differing degrees of accountability; and
4. Heavily dependent on the private sector for training, recruitment, and technology, leading to a high degree of informal interagency integration at the grassroots level.

The United States and Russia have clashed for years over what terminology to use: "information security," promoted by Russian officials, versus cyber, used by the United States. The Russian approach is more expansive and includes both psychological and technical elements, but essentially what the Kremlin means is control over online content — i.e., censorship.

2. History & Development

2.1. Origins

Today's Russian cyber command-and-control systems originated in the Soviet Union's signals intelligence (SIGINT) bureaucracy.

Throughout the Soviet period, two intelligence agencies were involved in breaking codes. The KGB had the 16th Directorate, in charge of intercepting and deciphering foreign communications. The General Staff of Armed Forces had the 8th Directorate and the Special Service of the GRU. Two agencies together ran Soviet SIGINT (which did not intercept text or speech but focused on identifying radio signals) and ELINT (which intercepted text and speech, i.e., content) centers abroad, including a facility at Lourdes in Cuba, which monitored and intercepted radio communications in the United States.[1]

Soviet military codebreakers were trained at the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko — the school was supervised by the 8th Directorate of the General Staff.[2] The personnel for the 16th Directorate of the KGB were taught at the KGB Higher School, the Fourth (Technical Department) in Moscow. The Fourth Department of the KGB Higher School had a better reputation and attracted students from three Soviet agencies that sent their recruits to study cryptography: the KGB, the Ministry of Defense, and the Ministry of Radioelectronic Production.

The KGB and GRU actively recruited talent from civilian universities known for their excellent math programs — the Moscow State University's departments of Physics and Math and Mechanics and Math (the latter had helped to form the Fourth Department of the KGB Higher School), Moscow Engineering Physics Institute (MEPhI), and Moscow Institute of Physics and Technology (MFTI or PhysTech).

This system largely survived the collapse of the Soviet Union.

2.2. The 1990s: The FAPSI Monopoly and Connection to the Cyber Industry

The KGB was restructured when the Soviet Union dissolved in late 1991. The 16th Directorate, along with several departments in charge of providing secure communications for party bosses, became the Committee of Government Communication. In December 1991, it was renamed as the FAPSI.[3] The idea was to create a Russian analogue of the US National Security Agency (NSA), but the FAPSI was also entrusted with conducting public opinion polls — for the Kremlin's eyes only — and, later on, with providing digital security for Russian elections.

1991 - 1999

Timeline of Russian Cyberwarfare Operations

1991 - The KGB is split into several agencies. The 16th Directorate, responsible for intercepting and deciphering foreign communications, becomes part of the Committee of Government Communication, later called the Federal Agency for Government Communications and Information (FAPSI). The 16th Directorate of the KGB is restructured as the 3rd Directorate of FAPSI, the main division of the organization in charge of spying on foreign telecommunications.

1992 - The 4th faculty of the KGB School is converted to the Institute of Cryptography, Telecommunications and Computer Science (IKSI) within FAPSI and directly continued the USSR model of recruiting and training intelligence agents.

1996 - The Educational and Methodological Association of Higher Educational Institutions on information security (UMO IB) is formed under the supervision of IKSI to develop and grow the cyber workforce, facilitating the recruitment of promising IT students to the cyber troops.

1998 - The FSB forms the first cyber unit within the agency – the Directorate of Computer and Information Security (UKIB).

1999 - The former head of FAPSI, Vladislav Sherstyuk, joins the Federal Security Council to manage cyber policy and establishes the Information Security Section.

1999 - Moonlight Maze investigation concludes that the first ever massive data breach of classified Pentagon and NASA documents was traced back to an IP in Moscow. In testimony before Congress, James Adams, CEO of Infrastructure Defense Inc, stated that, "the value of this stolen information is in the tens of millions, perhaps hundreds of millions of dollars."[1]

[1] United States Senate Committee on Governmental Affairs, Testimony of James Adams Chief Executive Officer of Infrastructure Defense, Inc., March 2, 2000

Credit: Dmitrii Melnikov / Alamy Stock Photo

The system of training and recruitment remained the same — the Fourth Department of the KGB Higher School, which was renamed as the Institute of Cryptography, Telecommunications and Computer Science (IKSI) within the FAPSI, and the FAPSI kept recruiting at MEPhI, MFTI, and Moscow State University. In 1996, the FAPSI sponsored the establishment of the Educational and Methodological Association of Higher Educational Institutions on Information Security (UMO IB) under the auspices of the IKSI.

The FAPSI was structured into six main directorates. The most important was the 3rd Directorate — the Main Directorate of Electronic Intelligence in Communications (Glavnoye Upravlenie Radioelectronnoi Razvedki Na Setyah Svyazi; GURRSS), in charge of spying on foreign telecommunications. The 3rd Directorate was the former 16th Directorate of the KGB.

Between 1995 and 1998, the 3rd Directorate was led by Vladislav Sherstyuk, a KGB officer since 1966 and a graduate of the Physics Department at Moscow State

University. Sherstyuk would play a major role in Russia's approach to cyber issues for decades.

Sherstyuk saw military action in the First Chechen War — he was put in charge of the FAPSI's task group deployed to Chechnya, and he organized the interception of the Chechens' communications.

In 1998, Sherstyuk was named head of the FAPSI.[4] The same year the FSB — the major domestic counterintelligence and counterterrorism agency — under the leadership of a new director, Vladimir Putin, entered the cyber field. In the Central Apparatus of the FSB, a new unit called the Directorate of Computer and Information Security (UKIB – Upravlenie Kompyuternoy I Informatsionnoy Bezopasnosti) was formed. It was subordinate to a larger department of counterintelligence. The UKIB was housed in a blockish, looming structure that was once the KGB's Computation Center, on the corner of Lubyanka Square and Myasnitskaya Street in Moscow. The FAPSI was headquartered in a stark, modern terraced building with giant antenna globes on the roof not far from Lubyanka Square, on Bolshoy Kiselny Lane.

In the Armed Forces, the General Staff's 8th Directorate was still operational, but it lacked resources. Both the FSB and the military's cyber capabilities were largely overshadowed by the FAPSI.

The early 1990s also saw the emergence of private cyber companies, like Kaspersky Lab, where the management had worked for the KGB. Kaspersky Lab CEO Evgeny Kaspersky himself had graduated from the Fourth Department of the KGB Higher School.[5] Thanks to their KGB background, those companies cultivated close relations with the security services and law enforcement agencies. What helped the FAPSI cultivate those relationships was that over the years the agency had been creating an industrial empire engaged in information security. The FAPSI was also in charge of licensing information security software — firewalls, cryptography, and so on — which meant that private companies needed to cooperate with it to get licenses.[6]

The period from 1998 to 1999 was probably the most influential time for the FAPSI.

In May 1999, Sherstyuk was transferred to the Security Council as its first deputy head. In December, he was appointed to preside over the information security section.[7] That section became the main unit where the cyber and information security concepts were implemented. One of the brains behind it was Anatoly Streltsov, a former KGB colonel.

Both Sherstyuk and Streltsov understood that they needed a research facility on cyber political issues that would help them engage in political decision-making on cyber. Thus, a department was created within Moscow State University under Sherstyuk

Photo: Moscow, Russia. 2 November 2018. Russian President Vladimir Putin addresses a gala event to mark the centenary of the Main Directorate of the General Staff of the Armed Forces of Russia known as the GRU at the Russian Army Theatre Credit: Planetpix/Alamy Live News

and Streltsov's supervision which soon became the Institute for Information Security Issues. This institute emerged as a major think tank that defined Russian foreign policy on information security.

In 2000, Sherstyuk and Streltsov's team composed the "Doctrine of the Information Security of the Russian Federation," which included a broad list of threats, ranging from "compromising of keys and cryptographic protection of information" to "devaluation of spiritual values," "reduction of spiritual, moral and creative potential of the Russian population," as well as "manipulation of information (disinformation, concealment, or misrepresentation)."[8]

Throughout the 1990s, the FAPSI and officials affiliated with it controlled the Russian cyber domain by training personnel, conducting operations, co-opting the private cyber industry, and establishing government cyber policies.

2000 - 2010

Timeline of Russian Cyberwarfare Operations

2000 - Vladimir Putin signs the “Doctrine of the Information Security of the Russian Federation.” The list of the country’s higher education institutions which provide training in information security is expanded.[2]

2003 - Vladimir Putin splits FAPSI between the FSB, SVR, and FSO. The 3rd Directorate of FAPSI, in charge of spying on foreign telecommunications, continues operation as the 16th Center of the FSB. The SVR sets up "Delta," a scientific production center to conduct research and development on cyber policy.

2004 - The UKIB is renamed as the Information Security Center of the FSB (TsIB). Vladimir Sherstyuk is downgraded to the position of Assistant to the Head of the Federal Security Council and is now dependent on the FSB's support to maintain connections to his former FAPSI departments.

2005 - The Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) is transferred to the Federal Technical and Export Controls Service. The Institute expands their work into cyber to "protect state secrets from foreign intelligence services via technical means."

2007 - After the Estonian government removed a Soviet war monument from downtown Tallinn, Russia-based attackers launch a series of denial of service attacks against Estonian public and private sector organizations. This is the first time that a foreign actor threatened another nation’s security and political independence through primarily cyber operations.

2008 - Two weeks before Russia’s invasion of Georgia, Russia-based attackers launch distributed denial of service (DDOS) to swamp and disable Georgian government websites.

2010 - The Association of Chief Information Security Officers (ARSIB) is launched. The ARSIB becomes the organizer of the Capture the Flag (CTF) competitions at schools and universities all over Russia as a recruitment mechanism for Russia’s intelligence community.

[2] Doctrine of Information Security of the Russian Federation approved by the President of the Russian Federation of September 9, 2000. N Pr-1895 https://base.garant.ru/182535/

2.3. The 2000s: The FSB Takes Over

2.3.1. Structural changes

The early 2000s saw a massive and rapid expansion of the FSB, including into the cyber arena.

On March 11, 2003, President Putin split the FAPSI between the FSB, the SVR, and the Federal Protective Service (FSO), in charge of providing protection for him and other high-level officials.[9]

Government communications and polling of public opinion were considered such a sensitive domain they were given to the FSO to supervise — and within that agency, the Service of Special Communication and Information (Sluzhba Specialnoy Svazyi I Informatsii; SSSI). The 3rd Directorate was moved to the FSB and became the 16th Center of the FSB (the Center of Electronic Intelligence in Communications). The regional ELINT units of the FAPSI were reorganized into the FSB Information Reception Centers.

In 2004, the FSB underwent administrative reform just like the rest of the federal agencies. Departments were renamed as services, and the UKIB was turned into the Information Security Center (TsIB or Centr Informatsionnoy Bezopasnosti) or the 18th Center of the FSB. The new center remained within the Service of Counterintelligence.

The FSB was divided into two large parts. The operations departments carried out counterintelligence, intelligence, counterterrorism, and other activities, whereas the support side of the organization included such activities as creating and providing special technical equipment and meeting other material needs. The TsIB was situated in the operations department, which was the most proactive. It was involved not only in the technical protection of computer networks but also in active operational surveillance, clandestine activity, and intelligence collection on the Internet. Inside the TsIB, the Operative Directorate was created to conduct operations.

The SVR founded a scientific production center, Delta, to conduct research and development (R&D) on cyber issues.[10] Delta was subordinate to the Directorate of Informatization of the SVR.

2.3.2. Cyber policymaking

Sherstyuk continued to define cyber policy while at the Security Council, the central body at the Presidential Administration responsible for managing the formulation and execution of security-related policies, though his position changed. In 2004, he was demoted to the position of assistant to the head of the Security Council. He

was forced to rely on the FSB's support since the most important departments of his former agency had been incorporated into the FSB. He also ensured the continued existence of the Institute for Information Security Issues at Moscow State University.

At the Foreign Ministry, Sherstyuk's team was supported by Andrei Krutskikh, an arms control talks veteran who shared Sherstyuk's approach to cyber issues detailed in the "Doctrine of the Information Security of the Russian Federation."[11]

The General Staff was sidelined by the FSB, which, for the most part of the 2000s, successfully rebuffed all attempts by the military to expand into the area of cyber.

2.3.4. Modus operandi under development

The 2000s were the period when the first cyberattacks took place beyond Russia's borders, including an attack on Estonia in 2007. Proxy groups affiliated with the Presidential Administration took responsibility for these attacks. APT29 or Cozy Bear — a Russian hacker group believed by Western cyber experts to be affiliated with either the FSB or SVR — was operational since at least 2008, according to Western experts.

2.3.5. Recruitment and training

The former FAPSI directorates, now within the FSB, continued recruiting from MEPhI, MFTI, and the Physics and Math Department at Moscow State University.

In training, the IKSI, previously within the FAPSI, was placed under the control of the FSB and became part of the FSB Academy.

The national program of training of civilian rank and file was significantly expanded: 73 Russian universities and high schools came to teach information security, united in the UMO IB. The chief institution supervising the association was the IKSI, which defined the UMO IB's requirements and guidelines. Of the 73 universities and high schools, only five institutions were military; the rest were higher polytechnic schools and state universities across the country.

Training in cyber followed the Soviet model of prioritizing loyalty and technical prowess over ethical considerations, resulting in an effective and devoted cyber workforce. After being recruited, students rarely, if ever, questioned why they were tasked with attacking Western or domestic targets, including Russian journalists and opposition politicians. Once again, the Soviet legacy is to blame. The Soviet Union had the biggest engineering community in the world because of its huge military-industrial complex — a collection of industries and research facilities which worked exclusively for the Soviet army and the KGB. To serve it, Josef Stalin founded dozens of technical schools all over the country. For many decades, Soviet

engineers were schooled intensively in technical subjects but rarely had exposure to the humanities. The scope of their education was exceedingly narrow. Unlike medical doctors who were trained in ethics, engineers were not. They were taught to be technical servants of the state. They were also taught secrecy since most of them were meant to work for the military-industrial complex of the KGB. As a result, generations of engineers were trained and worked their entire lives with little understanding of politics or trust of politicians and were suspicious of public activity as a whole. That system was never reformed after the collapse of the Soviet Union. After Putin became president, the Soviet approach to technical education based on secrecy and patriotism was only reaffirmed.

In addition, Russia's security services adopted a new tactic: approaching Russian criminal hackers and recruiting them. The FSB found itself in a good spot because the TsIB was tasked with prosecuting criminal hackers. Thus, they were able to give the hackers a choice: either join the FSB or go to prison. Of course, some accepted and even joined the TsIB.[12] The 2008 Russia-Georgia war only helped to solidify this new approach, but there are reports that some Russian hackers had been recruited even before the war.[13]

In 2009, the Education Ministry introduced a new educational standard that institutionalized "information security" as an area of study in Russian universities — cyber became a national priority in Russia's higher education.[14]

2.4. The 2010s: Explosive Growth

2.4.1. Structural changes

In 2012, Sergei Shoigu was appointed minister of defense. Ambitious and energetic, Shoigu wanted to prove himself as a military expansionist — cyber was a promising domain for increasing military influence. He also wanted his own cyber troops. He correctly identified the potential source of cyber personnel: the country's extensive network of technical universities.

In July 2013, Shoigu attended a meeting with Russian rectors at the Moscow State Technical University (MGTU) (one of the 73 educational institutions that provided training in information security) and told them of "a start of a major hunt for young programmers."[15] Later that same year, Russia's cyber troops were launched and advertised on YouTube, with the Kalashnikov rifle compared to a laptop.[16]

The Russian army still largely relied on the draft, and Shoigu tightened the rules for conscripts. It became impossible to avoid military service after graduating from college. When the cyber troops were launched, students in polytechnic universities were presented with a choice: either go to some distant army unit in Siberia or

2011 - 2016

Timeline of Russian Cyberwarfare Operations

2011 - Positive Technologies starts hosting hacker's CTF competitions, Positive Hack Days, which is also used by Russia's security services for talent recruitment. Digital Security company starts its own competition/conference for white-hat hackers, called ZeroNights, the same year.

2013 - The Ministry of Defense announces the launch of cyber troops with a Cyber command, although this change was never operationalized.

2014 - The list of Russian universities teaching information security expands to 170. The first military unit "research center" is launched at the Military Airforce Academy in Voronezh; soon after, more "research centers" are established.
The Ministry of Defense sets up the Special Development Center of the Ministry of Defense as a leading military cyber facility. The 85th Main Special Service Center (Military unit 26165 nicknamed Fancy Bear/APT28) within the GRU begins spotting talent in Russian schools, through collaboration with the FSB's IKSI.

2014 - Prior to the Ukrainian presidential elections, Russian hackers affiliated with the GRU's Main Intelligence Directorate carry out a series of cyberattacks to manipulate the vote. The CyberBerkut hackers invaded the network and deleted files in an attempt to change the election results by targeting Kyiv's Central Election Commission.

2016 - The FBI opens the "Crossfire Hurricane Investigation" amid increasing evidence and public discourse about Russian interference in the 2016 U.S. presidential elections through cyberespionage and information operations. The Russian intelligence community enters a period of internal turbulence as individual departments avoid responsibility for blowing cover.

2016 - The interference in the US election and the resulting backlash from the US intelligence community provoked a big internal crisis in Moscow where officials blamed each other for getting caught. The FSB's Information Security Center, in charge of counterintelligence, is decimated by internal purges.

join the cyber troops, where students were used to staff the so-called research companies (military units). The first "research company" was launched at the Military Airforce Academy in Voronezh – one of the five military schools on the list of 73 universities that were providing training in information security.

By 2014, the list of Russian universities teaching information security had expanded to 170.[17]

The Russian army skillfully exploited an old, outdated mechanism of draft to recruit the best and brightest among the Russian technical intelligentsia, sidelining the FSB. In the military, training in information security is supervised by the 8th Directorate of the General Staff in coordination with the Military Education Department of the Main Personnel Directorate of the General Staff.

The military also used other recruitment methods developed by the FSB — in 2015, the Capture the Flag (CTF) competitions run by the Association of Chief Information Security Officers (ARSIB, or Assotsiatsiya Rukovoditeley Sluzhb Informatsionnoy Bezopasnosti) got a new sponsor, the Special Development Center of the Ministry of Defense.[18] That center was launched by the Ministry of Defense in 2014 as a leading military cyber facility.[19] That same year, in December 2014, the 8th Directorate of the General Staff founded a research center on information security within the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko.[20] One of the "research companies" was based at the center and supervised by the 8th Directorate and the Science-Technical Committee of the General Staff — the main customers of R&D in the military.[21]

2.4.2. Cyber policymaking

The old guard led by Sherstyuk and Krutskikh still controlled Russia's cyber policy domain, but new actors came into play. First, the FSB delegated the head of the Science-Technical Service (NTS), Nikolai Klimashin, to the Security Council. He replaced Sherstyuk who remained active through his position at the Institute for Information Security Issues at Moscow State University. Klimashin did not have a background at the FAPSI, but he was chosen to supervise the liquidation and absorption of the FAPSI in 2003 (Putin wanted to have just one major intelligence/security agency — the FSB — not a competition of several agencies which his predecessor, Boris Yeltsin, had encouraged). As a result, Klimashin's NTS now included a department of the absorbed FAPSI, the Main Directorate of Security of Communications (GUPS), which became the 8th Center of the FSB or "the Center for Information Protection and Special Communications."

The General Staff of the Armed Forces became engaged in the cyber policy debate. One of the leading military cyber experts was Sergey Komov, himself a product of

Photo: Director of Russian Federal Security Service (FSB) Alexander Bortnikov and Director of Foreign Intelligence Service (SVR) Mikhail Fradkov arrive for a wreath-laying ceremony marking the 75th anniversary of the Nazi German invasion, by the Kremlin walls in Moscow, Russia, June 22, 2016. Credit: REUTERS/Grigory Dukor

military SIGINT training (Komov attended Kyiv's military radio-technical school and Govorov's military radio-technical academy in Kharkiv).

Since the early 2000s, Infoforum, a major Russian cyber conference, has been held in Moscow and later in the other regions. The General Staff has made sure to attend every Infoforum conference since 2013. As a rule, the head or deputy head of the 8th Directorate of the General Staff has been in attendance, sometimes accompanied by the head of the Military Science Committee of the General Staff.

The year 2016 saw the highest point of attention to cyber from the Kremlin. In February 2016, the Infoforum conference opened with a speech by Sergei Ivanov, then the chief of the Presidential Administration. "The powerful potential of such authoritative discussion platforms as Infoforum is fully engaged in solving the issues of ensuring information security," Ivanov said. Ivanov was a former general of the foreign intelligence branch of the KGB, a close associate of Putin's, and served

as minister of defense from 2001 to 2007. He was also reportedly one of the masterminds of the Russian interference in the US elections in 2016.[22]

On August 12, 2016, Ivanov was removed from his position as chief of Putin's administration (most likely because of the US outcry over the hacking of Democratic National Committee servers), but Putin preserved his seat on the Security Council.

Ever since, no Infoforum conference has been opened by the chief of Putin's Presidential Administration. It is quite likely that Putin no longer wants a direct connection between the Kremlin and a public cyber event.

2.4.3. Development of recruitment techniques

In 2010, a collection of private cybersecurity companies launched the ARSIB. The ARSIB was led by Victor Minin, a former officer of the KGB and FAPSI. The ARSIB runs the CTF competition at schools and universities in Russia. CTF is a massive, multiday hackathon in which one team defends its server as another team attacks it.[23] Minin told the authors of this report that the CTF competitions were seen by Russia's intelligence community as a perfect recruitment mechanism.

3. Russia's Evolving Cyber Command

3.1. Russia's Cyber Landscape after 2013

Throughout the turbulent period between 2013 and 2016, marked by Russia's invasion of Ukraine and illegal annexation of Crimea in 2014 and reckless interference in the US elections two years later, Russian cyber actors went through a series of crises brought on by the Kremlin.

By and large, the traditional actors, foremost the FSB, maintained a dominant role since they were well entrenched in the Russian security bureaucracy, including in positions on the Security Council, the Presidential Administration, and the Foreign Ministry.

Inside the FSB, the TSiB and the 16th Center remained the two most important cyber players.

In information sharing and recruitment/training:

- The TsIB was focused on using the connections between the vast Russian criminal hacking community and Russian private cybersecurity companies, including Kaspersky Lab. The FSB also made the TsIB a contact point with Western counterparts to share intelligence about Russian criminal hacker activity worldwide. The TsIB made amusingly good use of the shared intelligence. It tracked down Russian hackers and sought to recruit them.[24]
- The 16th Center relied on its significant cyber capabilities and recruited new talent in Russian polytechnic schools with courses in information security, supervised by the FSB's IKSI.

The head of the 16th Center, Sergey Buravlyov, held the position of deputy director of the FSB since 2005, and in 2013 he was promoted to the Security Council as deputy secretary, replacing Klimashin. Buravlyov was part of Sherstyuk's circle. Another one of Sherstyuk's protégés, Krutskikh, who had been serving at the Foreign Ministry, got a new position. In February 2014, Putin appointed Krutskikh as his special representative for international negotiations on Internet regulation.[25]

After the illegal annexation of Crimea in 2014, there was a significant and sudden increase in Russia's military cyber capabilities.

The Russian army found a way to boost its capabilities both in human resources and expertise. Rank and file were provided via the skillful use of the draft — students in Russian polytechnic schools joined Russian cyber troops in droves. The army also expanded training in cyber at military schools that taught personnel for SIGINT units

(in Russian terminology, radio technical intelligence, or OSNAS), like the Higher Military School of Radioelectronics in Krasnoyarsk.

Contracts were also granted to private cyber companies. In 2015, Kaspersky Lab's software was chosen by the Ministry of Defense as its primary antivirus solution. "By supplying the Kaspersky Business Space Security to the Russian Ministry of Defense through partners, we marked the beginning of a very important cooperation for us," said Sergey Zemkov, managing director of the Russian office of Kaspersky Lab at the time.[26]

The interference in the 2016 US elections (APT29 and APT28) and the resulting backlash from the US intelligence community created a crisis in Moscow where officials blamed one another for getting caught. The TsIB was decimated as a result of purges. Two senior TsIB officers were arrested on charges of treason. The head

2017 - 2022

Timeline of Russian Cyberwarfare Operations

2017 - A series of powerful malware attacks, known as NotPetya, swamp the websites of Ukrainian organizations including banks, government ministries, electricity firms, and newspapers. The attacks, which were disguised as ransomware but designed to cause maximum damage, are later traced to the Kremlin.

2017 - Two days before the final vote in the French presidential election, Russian hackers leak movre than 15GB of stolen data, including 20,000 emails, from Emmanuel Macron's campaign staff.

2018 - The National Computer Emergency Response Team is built within the 8th Center of the FSB, called The National Coordination Center on Computer Incidents, as a contact point with law enforcement cooperation in cyber. The massive Expert Intelligence Academy (ERA) Technopolis in the Krasnodar, run by the military, becomes operational. Eight "research companies' are transferred to the ERA Technopolis.

2020 - Russian state-affiliated hackers breach the SolarWinds Orion system, resulting in one of the biggest cybersecurity breaches of the 21st century. Using a supply chain attack, the hackers infiltrated several US agencies, including parts of the Pentagon, the US government departments of Homeland Security, State, Commerce and Treasury, and high-profile private companies such as Microsoft, Cisco and Intel.[3]

2021 - The Russia-affiliated Darkside hacking group attacks and shuts down the Colonial pipeline, disrupting the flow of nearly half of the total gasoline, diesel, and jet fuel used on the East Coast of the United States.

2022 - In the months leading up to Russia's invasion of Ukraine, Russia launches a series of distributed denial of service (DDoS) attacks against Ukrainian banking and government websites, some of which are attributed to the Russian Main Intelligence Directorate (GRU).[4]

[3] Saheed Oladimeji and Sean M. Kerner, "SolarWinds hack explained: Everything you need to know," Techtarget, June 29, 2022 https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[4] Foreign, Commonwealth & Development Office. "UK Assesses Russian Involvement in Cyber Attacks on Ukraine." GOV.UK. GOV.UK, February 18, 2022. https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine.

of the investigations unit at Kaspersky Lab and the head of the TsIB were forced to resign. The head of the TsIB's deputy also lost his job.

In January 2017, Buravlyov was quietly removed from the Security Council. Contrary to all Kremlin rules, no public announcement was made about his resignation. Buravlyov was replaced by Oleg Khramov, a brutal FSB general with no background in cyber but with experience conducting offensive operations in Ukraine. Apparently, both the TsIB and Buravlyov, who maintained officially sanctioned contacts with Western counterparts, fell victim to the Kremlin's paranoia.

As a contact point with Western powers, the TsIB was replaced by the 8th Center of the FSB. A national computer emergency response team (CERT), called the National Coordination Center on Computer Incidents, was built in the 8th Center. The 8th Center also originated from the FAPSI, but it was part of the NTS of the FSB; thus, it was not on the operational but rather the support side of the FSB.

Of the two cyber actors within the FSB, the 16th Center (dubbed Berzerk Bear, Dragonfly, and Energetic Bear by Western cyber researchers) emerged as a primary cyber offensive unit. In 2021, US authorities accused three officers of the 16th Center of sending fake e-mails with infected attachments to energy, including nuclear, companies in the United States between 2012 and 2017. According to the indictment, the three officers used spearphishing attacks that targeted more than 3,300 users at more than 500 US and international companies. They also targeted US government agencies such as the Nuclear Regulatory Commission.[27]

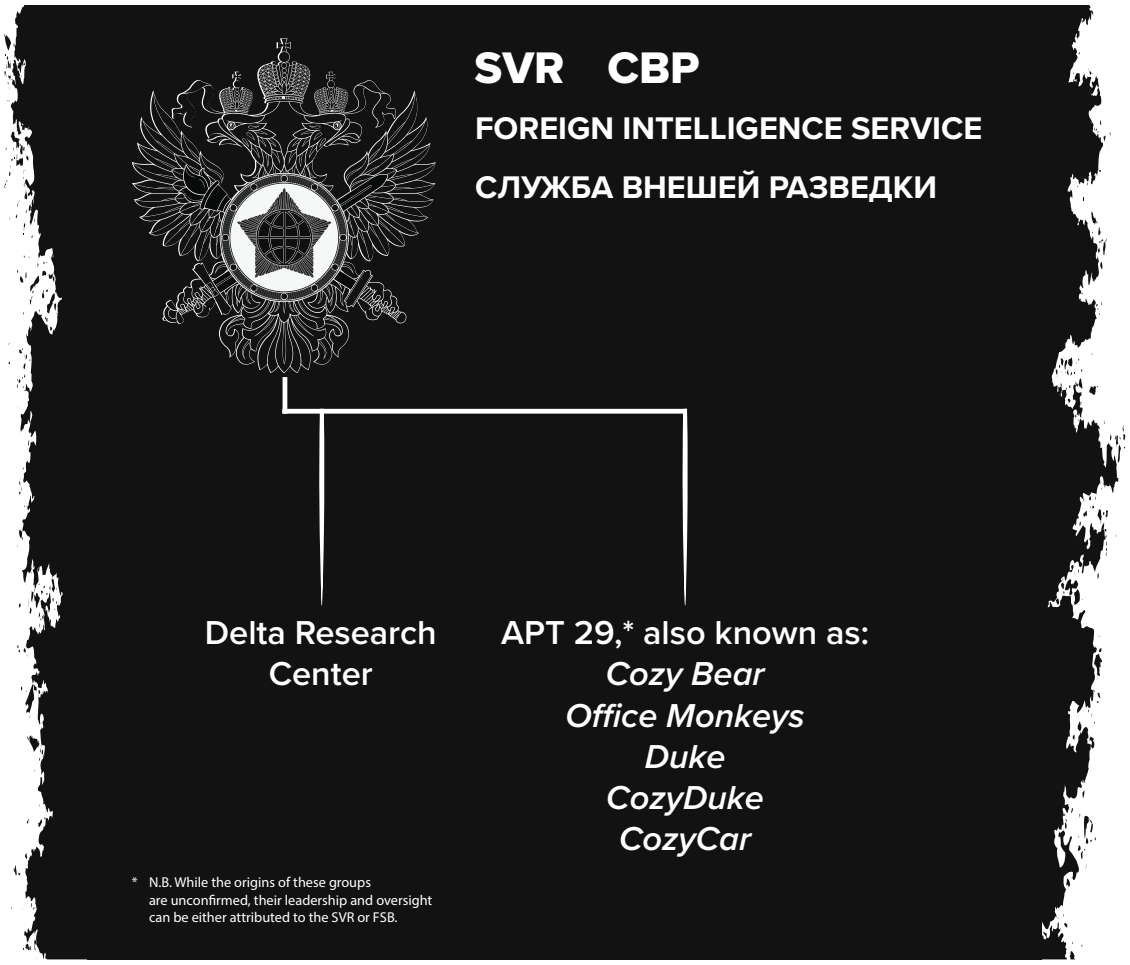
3.2. Military's Cyber Activities

3.2.1. Further expansion of the military

In recent years, the Ministry of Defense has built grand new facilities, like the buildings of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko and the Elite of the Russian Army (ERA) Technopolis in the Krasnodar region, operational since 2018.

The ERA Technopolis houses eight "research companies," including the "first research company" launched within the Military Airforce Academy in Voronezh — one of the five military schools on the original list of 73 educational institutions providing training in information security. The Advanced Research Projects Foundation (FPI), established in 2012 as a Russian analogue of the US Defense Advanced Research Projects Agency (DARPA), was also partly relocated to the ERA.[28]

The Ministry of Defense also found a new use for the military research facilities not previously associated with cyber.



The Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) has been the major research institution in the Russian military-industrial complex since before the Russian Revolution of 1917, involved in development and production of gunpowder, ammunition, and explosives for the army (in the Soviet Union it was known as NII-6). In 2005, the TsNIIKhM was subordinated to the Federal Technical and Export Controls Service in charge of protecting state secrets from foreign intelligence services via technological means. "This decision was the reason for a radical restructuring of this work, including the organization of new areas of scientific research," TsNIIKhM's website declared.[29]

On October 23, 2020, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) designated the TsNIIKhM, pursuant to Section 224(a)(1)(A) of the Countering America's Adversaries Through Sanctions Act (CAATSA), for knowingly engaging in significant activities undermining cybersecurity against any

person, including a democratic institution, or government on behalf of the Russian government.[30] The TsNIIKhM was found responsible for building a customized tool that enabled the August 2017 cyberattack on a Middle Eastern petrochemical facility.[31] The TsNIIKhM developed the Triton malware, also known as TRISIS and HatMan, to target and manipulate Industrial Controls Systems (ICS) that are used in some critical infrastructure facilities. The TsNIIKhM deployed the malware through phishing that targeted the petrochemical facility.

On the operations side, the 85th Main Special Service Center (Glavny Tsentr Specialnoy Sluzhbi; GTsSS), or military unit 26165 (dubbed Fancy Bear, APT28, or Strontium by Western cyber researchers) emerged as the main offensive facility of the Main [Intelligence] Directorate of the General Staff, along with military unit 74455.[32] In the Soviet Union, that center was part of the GRU's radio technical intelligence, or SIGINT; it was updated in the 2000s.

The GTsSS has been recruiting new talent in Russian schools since at least 2014 via cooperation with the FSB's IKSI.[33] It also recruits at hackers' conventions (see below). At least one officer of that center, Aleksey Morenets (wanted by the FBI since 2018), graduated from the Military Airforce Academy in Voronezh.[34] There is also 18 TSNII (Central Research Facility), or military unit 11135, operational since 1938, which has been involved in SIGINT/ELINT research, including "developing the equipment for conducting and coding satellite reconnaissance activities," and is now involved in information security under the auspices of the Main [Intelligence] Directorate.

The supervision of the cyber units in the military stayed the same — the 8th Directorate, the Main [Intelligence] Directorate, and the Science-Technical Committee, all at the General Staff of the Armed Forces.

3.2.2. Military setbacks

As early as March 2012, Russian Deputy Prime Minister Dmitry Rogozin spoke of the need to create a Russian military cyber command.[35] In February 2013, Shoigu announced his intention to create a cyber command and ordered the General Staff to provide him with recommendations. The defense minister set an end-of-2014 deadline.[36] However, the cyber command was never set up.

In 2017, Aleksander Sherin, deputy chair of the Duma's Committee on Defense, denied the existence of a cyber command and cyber troops in Russia.[37]

One of the reasons for this setback could be that the political decision-making in cyber is still dominated by the FSB (at the Security Council).

3.3. The Relationship between Russian Private and Security/Military Cyber Actors

Both the security services and the military have relied significantly on private actors to develop offensive cyber tools and conduct cyber operations.

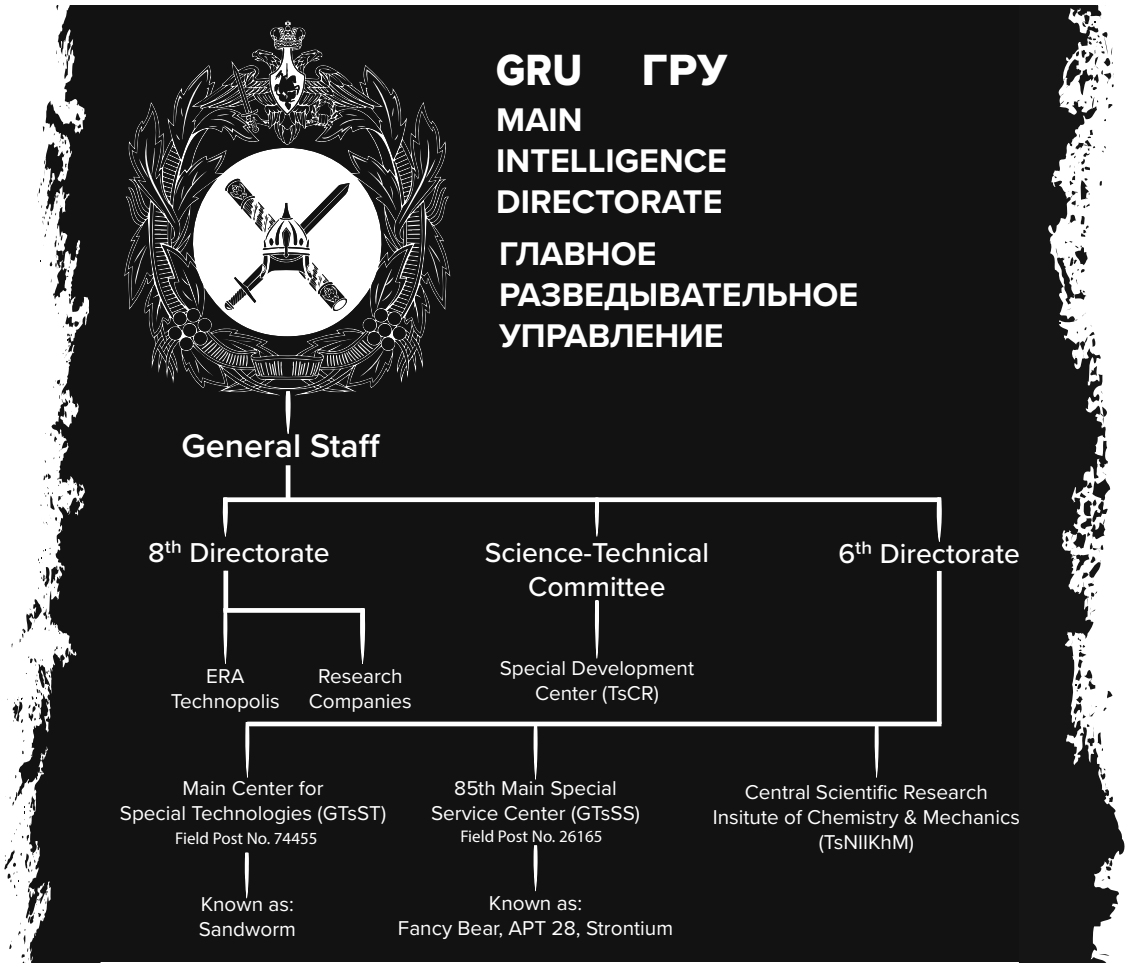
Russian state/private partnership in cyber works in several ways.

3.3.1. Partial privatization of the networks of R&D facilities inherited from the KGB

Russian security agencies and the military rely on an empire of research institutions they had built in Soviet times. In the Soviet Union, a significant effort was made to hide and disguise the true affiliation of these research institutions. Take, for example, the Scientific Research Institute of Dalny Svyazi, or of long-distance communications, in St. Petersburg, known as Dalsvyaz. The institute, with a staff of more than 10,000, was overseen by the Ministry for Industrial Telecommunications, but its real purpose was to work for the military. The offices of the applied acoustics unit (working on voice and speaker recognition) of Dalsvyaz were always guarded by men with automatic weapons because the unit was not under the control of the institute at all but was instead run by the KGB. It was a classic Russian matryoshka — secrets within secrets.[38]

Many of those research centers survived the collapse of the Soviet Union, like the Kvant Scientific Research Institute, founded in 1978 as a laboratory within the Design Bureau of Industrial Automation of the Ministry of Radio Industry. The ministry was officially civilian, but the Design Bureau of Industrial Automation was part of the Soviet military-industrial complex, while the Kvant laboratory was under the KGB. Kvant developed computers for the 16th Directorate of the KGB. It remained under control of the FAPSI in the 1990s and went to the FSB in the 2000s. At present, Kvant develops cyber weapons for the 16th Center of the FSB, essentially the same organization the institute has been working for since the beginning. The Design Bureau of Industrial Automation also remains active — now it's part of the Rostech empire and involved in developing drones.[39]

What has changed is that Kvant has launched private entities to work on FSB contracts. One of them is SyTech, a small company which has worked on contracts for the 16th Center since 2009, including a project for collecting data about users of social media (such as Facebook, MySpace, and LinkedIn), a project for deanonymizing Tor traffic with the help of rogue Tor servers, and a project to covertly penetrate P2P networks, like the one used for torrents.[40] On the surface, SyTech is a private company, but it shares personnel and contracts with Kvant (under US sanctions since June 11, 2018).[41]



This same approach is being used by the SVR. The agency has worked with private entities like AO Pasit, affiliated with the SVR, on SVR contracts using its scientific production center "Delta" as a customer.[42]

3.3.2. The role of private cybersecurity companies in recruitment and developing tools

The Russian company Positive Technologies identifies vulnerabilities in networks and publishes highly regarded research.[43] In April 2021, the company was blacklisted by the US Treasury for supporting the FSB.[44] According to the US Treasury, "Positive Technologies provides computer network security solutions to Russian businesses, foreign governments, and international companies and hosts large-scale conventions that are used as recruiting events for the FSB and GRU." The company said these were "groundless accusations," while its chief operating officer, Maxim

Photo: A poster showing six wanted Russian military intelligence officers is displayed as U.S. FBI Special Agent in Charge of the Pittsburgh field office Michael Christman, accompanied by Assistant Attorney General for the National Security Division John Demers, and FBI Deputy Director David Bowdich, speaks at a news conference at the Department of Justice, in Washington, U.S., October 19, 2020. Credit: Andrew Harnik/Pool via REUTERS

Pustovoy, said the blacklisting was based on "a misunderstanding and a mistake."[45] Positive Technologies has organized hacker competitions — Positive Hack Days and The Standoff — since 2011.[46] These events have been organized very much like the ARSIB's CTF competitions, used by the FSB to approach and recruit young talent (Kaspersky Lab also sponsored Positive Hack Days).[47] An officer of the 85th Main Special Service Center (military unit 26165) of the Russian military intelligence — Dmitriy Badin (wanted by the FBI since 2018) — took part in Positive Hack Days in 2014.[48] The same conference was also attended by officers of the FSB.[49]

Senior managers of Positive Technologies attended Infoforum conferences since at least 2013 and spoke alongside Krutskikh and officers of the FSB. Since 2014, Positive Technologies has sponsored Infoforums.[50]

Another Russian company, also blacklisted by the US Treasury, is Digital Security, a cyber research group. According to the US Treasury, "Digital Security worked on

a project that would increase Russia's offensive cyber capabilities for the Russian Intelligence Services, to include the FSB."[51]

What Positive Technologies and Digital Security have in common is that their business is identifying vulnerabilities in networks. Digital Security, however, has also held a competition/conference for white hat hackers, called ZeroNights, since 2011.[52] So those companies not only develop tools for Russian security services but also provide them with recruiting opportunities.

Digital Security's founder, Ilya Davidovich Medvedovsky, also co-wrote a book, *Attack on the Internet*, with two others, including a leading professor of information security at Peter the Great St. Petersburg Polytechnic University.[53]

3.3.3. The challenge of linking cyberattacks to the SVR

The SVR is an ambitious and capable intelligence-gathering agency. For several years, Western cyber experts attributed cyberattacks on Western targets to the SVR (in particular, the attacks carried out by APT29). However, unlike other Russian agencies, such as the FSB and GRU, where attribution was verified independently by Russian and Western investigative journalists, no details that would help link cyberattacks to a particular unit at the SVR or expose the chain of command inside the agency were ever found.

A real-life story: a Russian hacker's career in the year 2020

A young man in his early 20s, originally from an eastern suburb of Moscow, was a student at Bauman Moscow State Technical University. His father, a trained engineer, was a manager in a small private company, and his mother was an accountant. The young man was about to be conscripted to the army — a problem which all young men faced in Russia. Since the student studied computer science and information systems at the university — much like many other students — he was given a choice: either serve a year in a military unit located far from Moscow and live in the barracks; or join the cyber troops, stay in Moscow, share a room with another student, and visit family every weekend. A small salary for his service was also included. The young man did not hesitate. He decided to join the cyber troops, as did many of his peers, and stayed in Moscow. When he had finished his time in the army, the FSB offered him a job. He agreed, which surprised even his parents. His father asked him: Do you realize you won't be able to travel abroad? I don't really care, he responded.

4. Conclusions and Recommendations

As the world has seen in Ukraine, the Soviet military-industrial complex is back with a vengeance — only now, it is supplemented with cyber capabilities.

What we know about operational command and control in Russian cyber is limited, but as the history and analysis above has shown, we can draw four important conclusions.

First, Russia does not have a true cyber command. While the Presidential Administration and the Security Council coordinate cyber operations involving various agencies and non-state or quasi-state actors, they are not a cyber command in the US sense. There is no clear delineation of operational responsibility and no uniform system of reporting and accountability. Rather, Russia's cyber-active agencies and actors are governed through a largely informal system of relationships in which political expediency may trump operational efficiency.

Second, the organizational, strategic, and cultural differences that characterize Russia's various military and security agencies in the conventional field do not carry over into cyber operations. While their leadership may prefer not to, agencies such as the SVR and the GRU often find themselves attacking domestic cyber targets, while the FSB is active internationally.

Third, the lack of a true cyber command appears to mean that agencies tend to apply conventional approaches to cyber, rather than developing command-and-control approaches tailored to the cyber domain. While it is not clear that this has an adverse impact on efficacy, it further distinguishes patterns of cyber command in Russia from those found in the West. US and Western analysts must thus be careful not to assume that Russian structures and approaches mirror their own.

Fourth, Russia's cyber-active state, quasi-state, and non-state cyber actors share roots in the Soviet and early post-Soviet SIGINT and cyber spheres — roots that continue to shape how Russian cyber functions to this day. This is reflected in the significant and continuing dependence of state actors on the private sector for recruitment, training, and technology, and in the fact that all actors recruit broadly from the same cohorts of specialists, with operatives sometimes moving fluidly from one agency to another. In that sense, structural distinctions between Russian cyber actors may be misleading.

In the cyber arena, Russia's biggest asset remains its cadres. The Soviet Union boasted the biggest engineer community in the world to serve its enormous military-industrial complex. Under Stalin, dozens of polytechnic schools were built across the country to train engineers, and networks of research facilities — secret

and within the ostensibly civilian institutions — were funded for those engineers to contribute to the Soviet military and security services' R&D.

When the Soviet Union collapsed, this sprawling system shook but didn't break down. Some parts remained in the now independent countries, some fell into complete disarray due to lack of funding, but by and large, the parts within Russia survived the shock of the Soviet disintegration. The system did, however, experience a large hemorrhage of talent — many engineers went outside the tightly controlled world of the military-industrial complex to start a new life in private industry. Those engineers who chose the bright side launched Russian tech companies, including cybersecurity companies. The engineers, and their children, who chose the dark side, contributed to the emergence of the phenomenon of Russian hackers.

Under Putin, Russia's intelligence community and the military were given political and financial resources to make use of that legacy. The polytechnic schools were given resources to reproduce talent, and new recruitment practices were adopted to make good use of those human resources which had gone private — both in the legal cyber business and in criminal hacker activities.

These days, Putin's Kremlin relies on substantial cyber resources and a Soviet engineer culture that makes sure that enough talent and resources are available for Russia's cyber operations on a global scale. The IT talent exodus from Russia is still underway, and the organizational competition for this talent between the services will likely only intensify, but there is not yet any indication that this has diminished or will diminish the threat posed by Russia's cyber capabilities.

At least two things must be done to help contain the cyber threat from Russia.

Over the years, Western intelligence agencies accumulated substantial information about Russia's cyber efforts. More of this data should be made available to the public, including information about the command-and-control systems, especially of the SVR. Greater transparency is needed, and intelligence sharing on key actors and their activities must be made a priority. Also, more transparency would help formulate more rigorous export controls to ensure Western tech is not enabling R&D of Russian cyber offensive operations.

The issue of Russian engineer training should also be addressed. In the foreseeable future, one cannot hope that Russian authorities will start a proper reform of the Russian education system. But Russian IT engineers and programmers are an essential part of the global effort in technology development; this is one of the achievements of globalization. It would be useful to set up STS (Science, Technology, and Society) courses, similar to the ones at the best

US engineering schools, for Russian engineers working at Western companies. Educating Russian IT engineers on ethics would help bring a concept of the rule of law in the constantly changing world of cyber where the Russians are destined to play a key role no matter what political regime is in place in Moscow.

Endnotes

1 John Pike and Steven Aftergood, "Lourdes Signals Intelligence facility," *Federation of American Scientists Intelligence Resource Program*, October 18, 2001, https://irp.fas.org/imint/c80_04.htm.

2 "Eighth Directorate of the General Staff: State Secret Protection Service of the Armed Forces," Global Security, https://www.globalsecurity.org/intell/world/russia/8gumo.htm.

3 Andrei Soldatov and Irina Borogan, "The Dawn of a New Era: The Birth of the FSB," in *The New Nobility: the restoration of Russia's security state and the enduring legacy of the KGB* (New York: PublicAffairs, 2011), page 13.

4 Andrei Soldatov and Irina Borogran, "Putin's Overseas Offensive," in *The Red Web: The Kremlin's Wars on the Internet* (New York: PublicAffairs, 2017), page 225.

5 Loren Graham, *Lonely Ideas: Can Russia Compete?* (MIT Press, 2013), page 93

6 Gordon Bennet, "Boris Yeltsin's Favourite Agency," *The Federal Agency of Government Communications and Information*, Conflict Studies Research Center, August 2020, page 11, https://www.files.ethz.ch/isn/96806/00_Aug.pdf.

7 Andrei Soldatov and Irina Borogan, "How Putin Tried to Control the Internet," *Vice*, October 13, 2015, https://www.vice.com/en/article/gvyzn4/how-putin-tried-to-control-the-internet.

8 "The Government of the Russian Federation, Information Security Doctrine of the Russian Federation (Доктрина информационной безопасности Российской Федерации), " September 9, 2022, *Public Intelligence*, https://publicintelligence.net/ru-information-security-2000/

9 Gordon Bennett, "FPS & FAPSI - RIP," *Conflict Studies Research Centre*, March 17, 2003, https://www.files.ethz.ch/isn/96240/03_Mar_2.pdf.

10 Dmitry Medvedev, "Decree of the Government of the Russian Federation, July 18, 2016, N 1528-r (Докипедия: Распоряжение Правительства РФ от 18 июля 2016 г. N 1528-р)," *Dokipedia*, July 18, 2016, https://dokipedia.ru/document/5329851

11 The PIR Center, "PIR Center holds a press conference on 'Information Challenges for National and International Security' at the Press Center of the Russian Foreign Ministry," October 3, 2001, http://www.pircenter.org/news/352-20011003.

12 Dmitry Dokuchaev, aka Forb, for instance, was recruited by the TsIB as early as in 2006. He was arrested in 2016 on treason charges and released in 2021.

13 Daniil Turovskyy, "Psycho, Bold and other main cybercriminals of the Planet: Daniil Turovskyy tells how US intelligence agencies are hunting Russian hackers (Псих, Смелый и другие главные киберпреступники планеты Даниил Туровский рассказывает, как спецслужбы США охотятся за российскими хакерами)," Meduza, September 15, 2017 https://meduza.io/feature/2017/09/15/psih-smelyy-i-drugie-glavnye-kiberprestupniki-planety

14 "Order of the Ministry of Education and Science of the Russian Federation, October 28, 2009, No. 496 (Приказ Министерства образования и науки Российской Федерации от 28.10.2009 № 496," *Sbornik-Zakonov*, October 28, 2009, http://sbornik-zakonov.ru/35165.html.

15 Sergey Popsulin, "Sergei Shoigu announced a 'big hunt' for young programmers," *CNEWS*, July 4, 2013 https://www.cnews.ru/news/top/sergej_shojgu_obyavil_o_bolshoj_ohote

16 Daniil Turovsky, "Russian armed cyberforces: How the state creates military detachments of hackers (Российские вооруженные киберсилы Как государство создает военные отряды хакеров)," *Meduza*, November 7, 2016 https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily

17 "Infoforum 2014," *National Forum on Information Security*, 2014, https://old.infoforum.ru/conference/conference/view/id/5.

18 "Moscow Student Interuniversity Competitions on Information Security," M*oscow Capture the Flag*, 2015, http://mctf.aciso.ru/2015.html.

19 Daniil Turovsky, "Russian armed cyberforces: How the state creates military detachments of hackers (Российские вооруженные киберсилы Как государство создает военные отряды хакеров)," *Meduza*, November 7, 2016 https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily

20 Ministry of Defense of the Russian Federation, accessed June 24, 2022, https://function.mil.ru/news_page/country/more.htm?id=12203742@egNews.

21 Ministry of Defense of the Russian Federation, accessed June 24, 2022, https://function.mil.ru/news_page/country/more.htm?id=12203742@egNews.

22 Andrei Soldatov and Irina Borogran, "The Red Web Comes to the United States," in *The Red Web: The Kremlin's Wars on the Internet* (New York: PublicAffairs, 2017), page 328.

23 Association of Heads of Information Security Services. "Projects of the CTF movement in Russia (Проекты CTF-движения России)," accessed August 30, 2022, http://aciso.ru/aciso-projects/3861/

24 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

25 Andrei Soldatov and Irina Borogran, "Putin's Overseas Offensive," in *The Red Web: The Kremlin's Wars on the Internet*, (New York:PublicAffairs, 2017), page 237.

26 "Anti-Virus Defense of 'Kaspersky' in the Interests of the Ministry of Defense of the Russian (АНТИВИРУСНАЯ ОБОРОНА «КАСПЕРСКОГО» В ИНТЕРЕСАХ МИНИСТЕРСТВА ОБОРОНЫ РФ)," *DialogueScience*, September 15, 2011, https://www.dialognauka.ru/press-center/news/8323/?y=2021&m=03

27 Mike Eckel, "U.S. Accuses Three FSB Officers, Russian Ministry Programmer of Hacking Nuclear, Energy Firms," Radio Free Europe/Radio Liberty, March 25, 2022, https://www.rferl.org/a/us-indictment-hacking-fsb/31770359.html

28 "Ministry of Defense expects the active participation of the FPI in the projects of the ERA Technopolis (Минобороны ожидает активного участия ФПИ в проектах Технополиса «ЭРА»)," *TASS*, June 27, 2018 https://tass.ru/armiya-i-opk/5326608?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

29 "History of the Federal State Unitary Enterprise 'TSNIIKHM'," *The Federal State Unitary Enterprise TSNIIKHM*, accessed August 30, 2022, https://cniihm.ru/%d0%b8%d1%81%d1%82%d0%be%d1%80%d0%b8%d1%8f/

30 "CAATSA - Russia - related Designation," U.S. Department of the Treasury, October 23, 2022, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201023.

31 "Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," *U.S. Department of the Treasury*, March 31, 2022, https://home.treasury.gov/news/press-releases/jy0692.

32 "Russian Cyber Units," *Congressional Research Service*, February 2, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11718.

33 "In the footsteps of the officers. New details about the 'case of Russian hackers' (По следам офицеров ГРУ. Новые детали в 'деле русских хакеров')," *Radio Liberty*, July 17, 2018 https://www.svoboda.org/a/29372280.html

34 "Aleksei Sergeyevich Morenets," *Federal Bureau of Investigation*, accessed August 30, 2022, https://www.fbi.gov/wanted/cyber/aleksei-sergeyevich-morenets.

35 "The Ministry of Defense of the Russian Federation created troops of information operations (В Минобороны РФ создали войска информационных операций)," *Interfax*, February 22, 2017 https://www.interfax.ru/russia/551054

36 "Sergei Shoigu will continue to create a command for cyber warfare (С. Шойгу продолжит создание командования для ведения кибервойн)," *RBC*, February 12, 2013 https://www.rbc.ru/society/12/02/2013/570403629a7947fcbd44597d

37 "The State Duma denied the existence of «cyber troops» in Russia (В Госдуме опровергли существование «кибервойск» в России)," *Interfax*, January 16, 2017 https://www.interfax.ru/russia/545640

38 Andrei Soldatov and Irina Borogran, "We Just Come Up with the Hardware," in *The Red Web: The Kremlin's Wars on the Internet*, (New York:PublicAffairs, 2017), page 181.

39 "KRET electronics for drones will help in the development of the Arctic (Электроника КРЭТ для беспилотников поможет в освоении Арктики)," *Vzglyad-Info*, May 20, 2019 https://www.vzsar.ru/news/2019/05/20/elektronika-kret-dlya-bespilotnikov-pomojet-v-osvoenii-arktiki.html

40 Andrey Soshnikov and Svetlana Reiter, "Mosquito, Hope, Nautilus: hackers uncovered the essence of the projects of the FSB secret contractor (Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ)," *BBC*, July 19, 2019 https://www.bbc.com/russian/features-49050982

41 "Treasury Sanctions Russian Federal Security Service Enablers," *U.S. Department of the Treasury*, June 11, 2018, https://home.treasury.gov/news/press-releases/sm0410.

42 "Treasury Sanctions Russia with Sweeping New Sanctions Authority," *U.S. Department of the Treasury*, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0127.

43 Patrick H. 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/

44 "Treasury Sanctions Russia with Sweeping New Sanctions Authority," *U.S. Department of the Treasury*, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0127.

45 Alexander Marrow, "Defying US sanctions, Russian cybersecurity firm aims for 2022 IPO," *Reuters*, May 21, 2021 https://www.reuters.com/technology/defying-us-sanctions-russian-cybersecurity-firm-aims-2022-ipo-2021-05-21/

46 Maria Nefyodova, "Positive Technologies has published an open letter to the research community (Positive Technologies опубликовала открытое письмо исследовательскому сообществу)," *Xakep*, April 21, 2021 https://xakep.ru/2021/04/21/pt-open-letter/

47 "Sponsors," *Positive Hack Days*, 2015, https://2015.phdays.ru/about/sponsors/.

48 "Dmitriy Sergeyevich Badin," *Federal Bureau of Investigation*, https://www.fbi.gov/wanted/cyber/dmitriy-sergeyevich-badin; "In the footsteps of GRU officers. New details about the 'case of Russian hackers' (По следам офицеров ГРУ. Новые подробности «дела русских хакеров»)," *Radio Liberty*, July 17, 2018 https://www.svoboda.org/a/29372280.html

49 "Homepage," *Positive Hack Days*, 2014, https://2014.phdays.ru/

50 "Infoforum 2014," *National Forum on Information Security*, accessed August 30, 2022, https://old.infoforum.ru/conference/conference/view/id/5.

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

52 "International Conference on the Practical Aspects of Cybersecurity," *ZeroNights*, https://zeronights.ru/en/

53 Ilya Davidovich Medvedovsky, Pavel Valentinovich Semyanov and Dmitryy Gennadevich Leonov, *Attack on the Internet* (Moscow: DMK Press, 2020). https://www.litmir.me/br/?b=537193.

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
info@cepa.org | www.cepa.org

This report was funded by the Russia Strategic Initiative, US European Command. The views in expressed in this publication do not necessarily represent the views of the Department of Defense or the United States government.