CNA

AUGUST 2025

Hacking and Firewalls Under Siege

Russia's Cyber Industry During the War on Ukraine

Justin Sherman, Global Cyber Strategies

DOP-2025-U-042210-Final

CNA

Abstract

In this paper, we examine how Russian private sector cybersecurity firms are supporting the Russian government as well as how they have adapted to the new economic, security, and geopolitical environment since Russia's full-scale invasion of Ukraine in 2022. We describe the diversity of state and nonstate actors in Russia's cyber web—focusing on the role that private sector companies are playing in regard to cyber—and describe how relationships between state elements and cyber companies have changed over time. We provide case studies of three companies: Kaspersky, Security Code, and Positive Technologies. We analyze their relationships with the Russian government and how their functions tie into the Kremlin's objectives. We conclude with three questions that analysts, practitioners, and policy-makers should further explore to better understand the role of private cyber firms in Russia and to develop better responses to future Kremlin threats.

APPROVED FOR PUBLIC RELEASE. Unlimited distribution. **August 2025**

This report is part of a series generously funded by a grant from the Carnegie Corporation of New York.

This work was performed under Specific Authority Contract No. G-19-56503.

Cover image: Putin speaks at International Cybersecurity Congress, July 6, 2018. Russian Presidential Administration.

Approved by: **August 2025**

David Knoll, Research Program Director
Countering Threats and Challenges Program
Strategy, Policy, Plans, and Programs Division

Request additional copies of this document through inquiries@cna.org.

Executive Summary

Much of the Western analysis and commentary on Russian cyber threats since Russia's full-scale invasion of Ukraine in February 2022 have focused on state actors as well as some cybercriminal groups. However, another set of players has a key role in the Russian cyber ecosystem: private sector cybersecurity companies.

The Russian "cyber web" is complex, shifting, and often opaque, encompassing state-encouraged "patriotic hackers," independent developers, and state-recruited cybercriminal groups, among many other actors. The state does not control every actor—it could not control every single actor, in all ways, at all moments even if it wanted to do so. Entrepreneurialism, competition, and innovation abound in the Russian cyber web, too. Nonetheless, the state can coerce any actor at a single time and can use incentives, procurement contracts, and other mechanisms to compel them to behave in different ways. In this vein, the Russian government can and does draw on a spectrum of actors to assist with offensive, defensive, educational, recruitment, and other objectives related to cyber. The Russian government can use nonstate cyber actors to augment state capabilities, acquire new talent or services for the state, add a veneer of deniability to intelligence operations, and much more. Furthermore, security agencies such as the Federal Security Service (FSB), Foreign Intelligence Service (SVR), and military intelligence agency (GRU) have relationships with nonstate cyber actors that vary in structure and purpose over time.

Private cyber firms in Russia occupy an important role in this ecosystem. Although not every Russian cybersecurity firm is a government contractor, many firms provide services to the state. These services include supporting defensive operations, supplying defensive technologies, providing defense-oriented threat intelligence, identifying vulnerabilities to patch in Russian systems, offering open-source intelligence and reconnaissance services and technologies, identifying vulnerabilities for offensive operations, building exploits for offensive operations, assisting with offensive operations, cultivating talent, building propaganda-guided and national security–themed educational materials, and helping the security services recruit cyber talent. Some of these dynamics are not unique to Russia, such as a private company providing a state agency with firewalls. Other dynamics do stand out, such as the potential for the state to coerce a company or to carry out intelligence operations against dissidents or civilian critical infrastructure.

The Russian "cyber web" is complex, shifting, and often opaque, encompassing state-encouraged "patriotic hackers," independent developers, and state-recruited cybercriminal groups, among many other actors.

This paper offers case studies on three companies: Kaspersky, Security Code, and Positive Technologies. We analyze their relationships with the Russian government and how their functions tie into the

Kremlin's objectives. Kaspersky is a global company that has been repeatedly accused of quietly supporting Russian government cyber operations—including by allegedly using its antivirus platform to exfiltrate classified and sensitive information from other countries' systems. Security Code provides what appear to be principally defensive technologies and services to Russian customers, including the FSB, Ministry of Internal Affairs (MVD), Federal Protective Service (FSO), Russian Railways, Gazprom, and Sberbank. It also maintains educational partnerships with public and private institutions in Russia that train the future cyber workforce. Positive Technologies has been identified by the US government and in media reporting as a Russian intelligence contractor that supports offensive operations, reportedly by reverse engineering Western capabilities and turning vulnerabilities into exploits for offensive cyber operations. It also runs Russia's largest security conference and capture-the-flag hacking competition—an annual event that the FSB and GRU use to recruit highly talented hackers into the intelligence services.

Since February 2022, the three companies have been subject to additional levels of scrutiny, but they have adapted relatively well. Kaspersky went from being banned on US federal government systems to being sanctioned by the United States. It was also banned from providing many cyber products and services to American consumers and businesses, and it was identified by Germany, Poland, and others as a potential national security threat. But it has opened "transparency centers" in Latin America and elsewhere, which—contrary to what some in the West might expect—have paid off greatly for the firm as it has expanded. The company's marketing pitches seem to be landing well in many parts of the world, whether because of distrust of American technology post–Edward Snowden leaks, well-publicized abuses by Silicon Valley giants, or the mere fact that Kaspersky is a global firm with talented personnel. However, Kaspersky is now providing protections to a notorious Russian "bulletproof" web hosting provider for cybercriminals (meaning one that hides and refuses to disclose its customers, even to governments), marking a notable departure from its past efforts to portray itself as a trustworthy brand.

Security Code has been sanctioned by Ukraine and the United States but not by the European Union. It has also remained out of the Western press, perhaps because of its role in Russian cyberdefense rather than the much more headline-grabbing category of cyberoffense. In its 2024 financials, it disclosed that most of its clients are those protecting "critical information infrastructure," a Russian legal term for entities handling information systems, networks, and technologies that are critical to the state's security. As a result, most of Security Code's clients ostensibly reside in Russia. It appears that the company's bottom line is strengthening because of growing demands in Russia for cyberdefense amid the continued war.

Positive Technologies has been marketing itself as a way for entities in other countries to diversify their cybersecurity services. It does not suggest that countries forgo American, Chinese, or Israeli cyber providers; rather, it makes the case for adding a Russian vendor to avoid depending too much on one country for cyberdefenses. In addition, the company has launched new product offerings, and in-person attendance at its flagship conference (the event the FSB and GRU use to recruit personnel) has more than quintupled from 10,000 in 2022 to 55,000 in 2023, with another 100,000 tuning in online. All three of these companies—despite waves of Western sanctions, export controls, and technology isolation efforts—had their highest revenue figures ever in 2024.

Some of these firms (and others not covered in this paper) are directly supporting the Russian government's offensive cyber operations, making them direct security risks for the United States and

the West. Other firms may be providing defensive services, such as helping the Russian government and economically critical entities detect and mitigate intrusions from countries such as Ukraine. To understand the security implications of private companies working with the Russian government, we recommend that analysts, practitioners, and policy-makers consider three critical questions:

1. How can companies better identify Russian providers in supply chains and determine whether they present risks?
2. In which regions and markets are Russian cyber firms expanding the most, and what can their sales pitches and successes teach the United States and the West?
3. What would a more analytically robust, comprehensive assessment of possible Russian private company support for the Kremlin look like?

PAGE INTENTIONALLY BLANK

Table of Contents

PAGE INTENTIONALLY BLANK

Introduction

Much of the research and analysis of Russian cyber operations during Russia's war against Ukraine have focused on Russian state agencies. The principal agencies involved in cyber operations are the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the military intelligence agency (GRU). These agencies have supported destructive and disruptive wiper attacks on Ukrainian institutions and intelligence collection to enable Russian military strikes.[1] Furthermore, these agencies' cyber operations are persistent, sophisticated, well resourced, and, as a result, highly concerning for the United States and the West.

However, far less attention has been paid to the role of private sector companies in Russia that support Russian cyberdefensive capabilities and activities, cyberoffensive capabilities and activities (including exploit development), and a wide range of other state-driven cyber objectives, such as recruiting cyber personnel to the Russian intelligence community.

Through some of these activities, private sector companies may be directly enabling Russian security organizations to compromise foreign targets. Through others, they may be detecting and preventing attempted nation-state intrusions—or helping Russian state agencies to mitigate and recover from ongoing nation-state intrusions—into Russian systems.[2] The fact that the Russian government contracts with these private firms has many direct implications for the United States and the West regarding cybersecurity, national security, competition for tech market share in third countries (i.e., not Russia or the United States), and perceptions of Russia's technological and economic isolation from the rest of the world.

This paper proceeds in four parts. We first describe Russia's overall cyber ecosystem, including the number of actors within it and the complexity of the "cyber web," with a focus on the role of private sector companies. We then evaluate the state of Russia's private sector cyber industry ahead of Russia's February 2022 full-on invasion of Ukraine, and we provide case studies on three Russian government cyber contractors—Kaspersky, Security Code, and Positive Technologies—that allegedly or by their own admission support the state on cyber-related issues and activities, including exploit development, talent cultivation, and incident mitigation. In the third section, we analyze how Russia's cyber industry has adapted to the war by looking at the financial successes and business evolutions of the three companies since February 2022. We conclude with three questions that analysts, practitioners, and policy-makers should further pursue to better identify and mitigate national and economic security risks.

[1] See, for instance, Tom Balforth, "Exclusive: Russian Hackers Were Inside Ukraine Telecoms Giant for Months," Reuters, Jan. 5, 2024, https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/; "The GRU's Disruptive Playbook," *Mandiant*, July 12, 2023, https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook.

[2] Russian cyber firms would be defending against intrusions from Ukraine and also from the Chinese government, among others. See, for instance, Ronen Bergman and Kate Conger, "Chinese Hackers Tried to Steal Russian Defense Data, Report Says," *New York Times*, May 19, 2022, https://www.nytimes.com/2022/05/19/world/asia/china-hackers-russia.html.

Private Firms in the Russian Cyber Web

Russia's cyber web encompasses state and nonstate actors, including government agencies, "patriotic hackers" encouraged by the Kremlin, cybercriminals (including those hired by the security services and those acting independently), independent developers, private sector state contractors, and private military companies, among other actors.[3] In some countries, offensive cyber operations are primarily carried out by government agencies. By contrast, the Russian government can and does draw on a spectrum of actors to assist with cyberoffense, as well as cyberdefensive, educational, and other objectives. In this section, we characterize the Russian state's relationships with nonstate cyber actors, zoom in on private sector cybersecurity firms, and explain how those state-nonstate relationships vary by agency and over time.

In some countries, offensive cyber operations are primarily carried out by government agencies. By contrast, the Russian government can and does draw on a spectrum of actors to assist with cyberoffense, as well as cyberdefensive, educational, and other objectives.

The role of nonstate actors in Russian government cyber operations reflects the "violent entrepreneurship" that criminals, private firms, and other nonstate actors have participated in since the collapse of the USSR, a system in which private entities shape Russian markets through the management of violent crime and services (though in the cyber case, perhaps not literal violence).[4] Nonstate cyber actors compete with one another, sometimes aggressively, in a system that is subject to Kremlin directives but not to complete top-down control. They provide services that overlap with government services (e.g., offering armed protection or digital exploits) or go beyond them (e.g., offering business-to-business murder-for-hire or building commercial firewalls).[5] These nonstate actors often offer what their clients would consider genuinely useful capabilities and resources (e.g., racketeering-laden business security and ransomware-as-a-service platforms) and what the state would consider geopolitically useful

[3] See, for instance, Janne Hakala and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace*, NATO Strategic Communications Centre of Excellence, June 2021, pp. 17–22, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.

[4] Vadim Volkov, *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism* (Ithaca: Cornell University Press, 2016). Thanks to an individual who shall remain anonymous for initial discussion of this analogy in a 2022 workshop.

[5] Extra-governmental services include products such as Kaspersky's firewall. For information on the murder-for-hire business, see Sonni Efron, "Murder for Hire in Moscow: A Wave of Contract Killings Has Russians on Edge. Businessmen Are the Prime Targets of Brazen Hit Men, Who Style Themselves After American Gangsters," *Los Angeles Times*, Aug. 13, 1993, https://www.latimes.com/archives/la-xpm-1993-08-13-mn-23397-story.html.

tools.[6] Their activities range from legal (e.g., selling cyberdefensive services) to nominally illegal but tacitly permitted or influenced (e.g., cybercrime), or they may exist in a gray zone in direct service of the Russian state (e.g., cybercriminals taking on state-commissioned hacking projects). Russian President Vladimir Putin, for example, helped cultivate Russia's current cybercriminal ecosystem, illustrating that top-down forces coexist with competition and entrepreneurship.[7]

How Moscow uses nonstate cyber actors mirrors how it uses nonstate non-cyber actors for conflict and subversion, both during wartime and below the threshold of armed conflict. Just as the Russian military may use the motorcycle gang Night Wolves to help carry out *maskirovka* (military deception) activities—traditionally the remit of a state agency, in this case the GRU—the Russian security services may have private companies assist with offensive cyber operations against foreign targets that might otherwise be entirely led by a state agency.[8] Just as the Russian government may set up a fake private military company to recruit and deploy soldiers to Ukraine, agencies like the GRU may leverage supposed nonprofit and academic fronts to onboard talent and run cyber-enabled influence operations against the United States.[9] The Russian military and security services also view cyber operations and capabilities (what Russia sees as part of the expansive concept of "information security") as integral to their power projection and regime security efforts.[10] Hence, nonstate cyber actors are important to the Kremlin for national security reasons.

Private-sector cybersecurity firms occupy an often underappreciated role in Russia's cyber ecosystem. Although not every Russian cybersecurity firm is a government contractor, many firms provide services to the state, including supporting defensive operations, supplying defensive technologies, providing defense-oriented threat intelligence,

---

[6] Kurt Baker, "What Is Ransomware as a Service (RaaS)?," Crowdstrike.com, Jan. 30, 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/. For more on racketeering, see Volkov, *Violent Entrepreneurs*, p. 34 (quoting a study that found that "small entrepreneurs gradually established working relations with racketeers and, as interview sources indicate, viewed these relations as beneficial, given the existing business environment. They saw racketeers as providers of real services and demanded them when circumstances required").

[7] See, for instance, Lucie Kadlecová, "Russian-Speaking Cyber Crime: Reasons Behind Its Success," *European Review of Organised Crime* 2, no. 2 (2015), pp. 104–21, https://standinggroups.ecpr.eu/sgoc/wp-content/uploads/sites/51/2020/01/kadlecova.pdf; Justin Sherman, *Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior*, Atlantic Council, Sept. 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/.

[8] On the GRU, see Hakala and Melnychuk, *Russia's Strategy in Cyberspace*, p. 11. For more on reactions to Russian security services' actions, see US Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," Treasury.gov, Apr. 15, 2021, https://home.treasury.gov/news/press-releases/jy0127.

[9] On fake private militaries in Ukraine, see "How Russia's GRU Set Up a Fake Private Military Company for Its War in Ukraine," Radio Free Europe/Radio Liberty, Oct. 10, 2023, https://www.rferl.org/a/russia-gru-fake-private-military-company-ukraine-redut-investigation/32630705.html. For a prominent example of cyber-enabled influence operations against the US, see US Department of the Treasury, "Treasury Sanctions Entities in Iran and Russia That Attempted to Interfere in the US 2024 Election," Treasury.gov, Dec. 31, 2024, https://home.treasury.gov/news/press-releases/jy2766.

[10] For "information security," see Gavin Wilde and Justin Sherman, *No Water's Edge: Russia's Information War and Regime Security*, Carnegie Endowment for International Peace, Jan. 2023, https://carnegieendowment.org/research/2023/01/no-waters-edge-russias-information-war-and-regime-security?lang=en; Olga Chislova and Marina Sokolova, "Cybersecurity in Russia," *International Cybersecurity Law Review* 2 (2021), pp. 245–51, https://link.springer.com/article/10.1365/s43439-021-00032-9. Information concepts (and concepts of what Western audiences would call "cyber") are littered throughout various Russian military documents and doctrines, including Wilde and Sherman, *No Water's Edge*; and Michael Kofman et al., *Russian Military Strategy: Core Tenets and Operational Concepts*, CNA, DRM-2021-U-029755-1Rev, Oct. 2021, https://www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts.

identifying vulnerabilities to patch in Russian systems, offering open-source intelligence and reconnaissance services and technologies, identifying vulnerabilities for offensive operations, building exploits for offensive operations, assisting with offensive operations, cultivating talent, building propaganda-guided and national security–themed educational materials, and helping the security services recruit cyber talent. We highlight many of these services in the company case studies.

Some Russian government cyber contractors have ongoing state relationships. Other private sector Russian cyber firms may dip into state contracting for a brief period before returning to their private sector client base. The agencies procuring these services also vary, but the main ones are the FSB, GRU, SVR, and Ministry of Defense (MOD). Each of these organizations contracts with private sector Russian cyber companies, including for offensive purposes. But plenty of other Russian government agencies—including the Ministry of Internal Affairs (MVD) and the Russian Constitutional Court—depend on private sector cybersecurity contractors for firewalls, intrusion detection software, and other defensive technologies.[11] There is no one-size-fits-all relationship, temporally or functionally, between the "Russian government" and private sector cyber contractors.

We emphasize that a private sector cyber firm contracting for a government is neither unique to Russia nor inherently offensive. Work by scholars such as Tim Maurer, Michael Schmitt, Liis Vihul, Jon Lindsay, and Jason Healey has shown that many states engage in such practices and rely on private sector cyber proxies to perform core functions and expand their talent base.

We emphasize that a private sector cyber firm contracting for a government is neither unique to Russia nor inherently offensive. Work by scholars such as Tim Maurer, Michael Schmitt, Liis Vihul, Jon Lindsay, and Jason Healey has shown that many states engage in such practices and rely on private sector cyber proxies to perform core functions and expand their talent base.[12] As we have noted, this work does not have to be offensive. A state may turn to a private sector cybersecurity company for defensive technologies, enabling technologies (e.g., strongly encrypted and hardened infrastructure), collections and networks of talent, and expertise in niche subjects.

Even so, the Russian government's use of cyber contractors has implications for Western and US security. In the current Russian cyber ecosystem, Russian private sector firms are helping defend Russian government networks against Ukrainian

[11] See the case study on Security Code in the Building Up the Base section, p. 13.

[12] See Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Carnegie Endowment for International Peace, 2018; Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution," *Fletcher Security Review* 1, no. 53 (2014), pp. 54–73, https://ccdcoe.org/library/publications/proxy-wars-in-cyberspace-the-evolving-international-law-of-attribution/; Jon R. Lindsay, "Proxy Wars: Control Problems in Irregular Warfare and Cyber Operations," in *International Studies Association Annual Meeting*, Apr. 2013, http://files.isanet.org/ConferenceArchive/1a381131aa014f02ab15a7b55b8509d7.pdf; and Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council, Feb. 2012, https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

cyber intrusions and find vulnerabilities for Russian intelligence agencies to exploit abroad. In the most extreme cases, such private sector firms are participating in Russian cyber operations against Western targets. As a result, Russian private cyber contractors represent a security consideration for the West.

The Kremlin benefits from having a wide group of cyber actors to draw upon. Such actors offer the Kremlin deniability (even if implausible) for operations, the ability to locate their own technical operations and infrastructure outside of state hands (e.g., on private sector servers), a wide talent base, a wide set of capabilities (e.g., private sector and criminal innovation), and the freedom to leverage talent and capabilities on an ad hoc basis.[13] Since the outbreak of the war, many Russian technology companies have become more inclined to support state efforts in response to Russian propaganda promoting nationalism, securitization, and the narrative that the country is under assault by the West.

At the same time, drawing on private sector firms to augment cyber power is not without risk. Third parties can sometimes be unreliable or have underlying priorities (especially profit), and they can occasionally sell bad products deliberately.[14] In addition, following the government's invasion of Ukraine, private sector cyber firms have been hit with sanctions or affected greatly by attempts at economic and technological isolation, which has forced many to fight for their survival. These shifts have forced some Russian private sector cyber firms to shift their product and market focuses and, in some cases, have deprived them of access to Western technology and expertise—indirectly affecting the Russian government, too.

[13] Paul Stronski, "Implausible Deniability: Russia's Private Military Companies," Carnegie Endowment for International Peace, June 2, 2020, https://carnegieendowment.org/posts/2020/06/implausible-deniability-russias-private-military-companies?lang=en; Kevin P. Riehle, "Ignorance, Indifference, or Incompetence: Why Are Russian Covert Actions So Easily Unmasked?," *Intelligence and National Security* 39, no. 5 (Jan. 2024), pp. 864–78, https://www.tandfonline.com/doi/full/10.1080/02684527.2023.2300165.

[14] One of the prime examples of this in recent years may be the Russian intelligence contractor Vulkan selling the state on projects that purported to achieve outcomes such as influencing entire other populations' opinions. See, for instance, Craig Timberg et al., "Secret Trove Offers Rare Look into Russian Cyberwar Ambitions," *Washington Post*, Mar. 30, 2023, https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/.

Building Up the Base: Russia's Cybersecurity Private Sector Before 2022

Russia's cybersecurity sector has long had a global reach. Especially before the Putin regime's full-scale invasion of Ukraine in February 2022, many Russian cybersecurity companies were providing services to public, private, and nonprofit organizations in Russia and abroad. Some companies have little to no engagement with the government, even as they remain susceptible to its influence and coercion. Other companies have contracted and partnered with the Russian government to support offensive operations, identify vulnerabilities and develop exploits, provide defensive products and services, and train and educate future generations of the cyber workforce. Understanding how the Kremlin has interacted with a selection of cybersecurity companies in the past will help inform an analysis of—and potential responses to—Russian cyber actions in the future.

Understanding how the Kremlin has interacted with a selection of cybersecurity companies in the past will help inform an analysis of—and potential responses to—Russian cyber actions in the future.

In the following subsections, we examine private sector Russian cyber companies Kaspersky, Security Code, and Positive Technologies. We selected these three companies for their importance in the Russian cyber industry and their efforts to adapt to the war. They represent three types of companies: one with questionable involvement with the Russian state, one known to be supporting Russian government cyberdefense, and one known to be supporting Russian government offensive cyber operations and talent recruitment for security services.

Case study methodology

The examination of these companies was designed to answer three sets of questions: How do these companies work with the Russian government? What, if anything, do these companies say about their work with the Russian government, and how does it compare to what has been disclosed elsewhere, such as in the press or by the United States? Have the companies' engagements with the Russian government and public statements about those engagements changed since February 2022, and if so, how? The first two of these are principally addressed in the first sets of case studies in this section, scoped before February 2022, and the last of these is principally addressed in the subsequent report section, scoped after February 2022. These questions illuminate key issues at the center of Russia's cyber web and probe more deeply into the complexity of the Russian government's interactions with private sector cyber firms—and their combined threats to the United States and the West.

Methodologically, we strove to be as comprehensive as possible in describing these companies and their activities. To do so, we drew on Western scholarship, Western and Russian media stories and investigations, US and European government disclosures and sanctions designations, and open-source intelligence that we gathered from, among

others, the selected companies' websites and public-facing materials. Wherever possible, we sourced information from news articles, webpages, and so forth that were available online at the time of writing. Information is plentiful in some areas (e.g., reporting on Kaspersky, information on Security Code's clients).

As with any open-source research endeavor, however, available information is limited. First, the Russian government and Russian companies have strived to block access to or purge relevant material from the internet. The Russian government has taken significant steps since February 2022 to block Western access to Russian government websites. Russian government agencies have also removed, since February 2022, many documents, databases, and other kinds of content from websites that previously described topics and entities of relevance to this report, such as Russian cyber policy and Russian security agencies. Likewise, some of the companies covered in the case studies have imposed limits on the availability of their previously public materials, including materials describing their engagements with state agencies and their exact capability offerings. In these instances, we rely instead on archived online versions of the source materials, such as Internet Archive snapshots of company webpages describing engagements with the Russian government. All footnotes include hyperlinks to the underlying source materials to the extent possible, including when past versions of those source materials are archived online.

The second information limitation we face pertains not to blocked access or purged materials but to an absence of information in the first place. For instance, some of the private sector companies in the case studies make materials describing their work with specific Russian government agencies available but do not go into detail about the nature or the timeline of that work. None of the three companies break down their revenue by client, making it somewhat unclear how much money they make from working with specific state agencies. The companies do not provide detailed revenue breakdowns by country and region, either, impeding a full assessment of their market expansion efforts in the aftermath of the February 2022 invasion. In these instances, more information is needed to fill the gaps and better evaluate the companies' behaviors and the implications for US and Western security.

Case study #1: Kaspersky

Kaspersky is probably the most well-known Russian cybersecurity company. Eugene Kaspersky, a cybersecurity researcher, cofounded the company in June 1997.[15] In 1994, Eugene Kaspersky and four coworkers were working at system integration firm KAMI when they decided to launch a research and development initiative focused on computer viruses. By 1997, they had left KAMI, and Eugene Kaspersky and two others formally turned the R&D initiative into Kaspersky Labs.[16] Kaspersky signed its first large international contract with Finnish company F-Secure in 1998, opened its first international office in the United Kingdom (UK) in 1999, built its antivirus software for pocket computers in 2001, and opened offices in Japan, Germany, France, Spain, Italy, and China in 2003.[17] Natalya Kaspersky, a cofounder, commented later that the company had always had a bootstrapping mentality. More than a decade after

[15] Kaspersky, "Brief Company History," kaspersky.com, accessed Jan. 24, 2025, https://web.archive.org/web/20250124102647/https://esg.kaspersky.com/en/about-company/brief-history.

[16] *Global Entrepreneurship and the Successful Growth Strategies of Early-Stage Companies*, World Economic Forum, 2011, p. 191, https://www.iese.edu/media/research/pdfs/ESTUDIO-137.pdf.

[17] Kaspersky, "Brief Company History"; *Global Entrepreneurship*, p. 191.

the company's founding, she remarked that "we understood that the only chance in Russia to get the company financed at the time was through our own sales and profits; hence, the task to bring in new clients early on was our top priority."[18]

At its inception, the company had 13 employees and just 5 percent of the Russian antivirus market.[19] By 2000, it had 65 employees and controlled 60 percent of the antivirus market in Russia.[20] By 2014, it had more than 2,800 employees operating in almost 200 countries and territories, covering more than 300 million people.[21] Its revenue growth from 2009 onward, as captured in Figure 1, was considerable, increasing from $391 million in 2009 to $711 million just five years later. Kaspersky's revenue was also spreading far outside Russian borders, signifying its ascension to a global cybersecurity leader—58 percent of its 2016 revenue (roughly $374 million) came from business that Kaspersky conducted in the United States and Western Europe.[22]

Over time, and as Putin expanded his grip on the country (including on industry), Western policy-makers and analysts began to speak more about Kaspersky and whether its Russian headquarters and incorporation made it susceptible to the Russian government's influence.[23] To those following how Putin was cementing control, the answer was obviously yes.

Whatever the reasoning, be it "to help others," "security heads-up!," "hooliganism" or "criminal intent," hacking is a phenomenon which is deeply rooted in the world of computing and will probably never die. There will always be people immature enough to abuse public resources, self-proclaimed "Robin Hoods" and criminals hiding in the dark alleys of cyberspace.

"An Analysis of Hacker Mentality," Kaspersky IT Encyclopedia, 2004, https://web.archive.org/web/20241210093016/https://encyclopedia.kaspersky.com/knowledge/an-analysis-of-hacker-mentality/.

In July 2012, a story in *WIRED* alleged that Eugene Kaspersky and his company maintained a close relationship with the FSB. It claimed that when Eugene Kaspersky's son was abducted in April 2011, Eugene had his corporate security manager call the FSB. He then told *WIRED*, "We have very good

18 *Global Entrepreneurship*, p. 192.

19 *Contemporary Biographies in Communications & Media* (Englewood Cliffs: Salem Press, 2014), p. 110, https://web.archive.org/web/20150426074648/http://salempress.com/store/pdfs/bios_com_pgs.pdf.

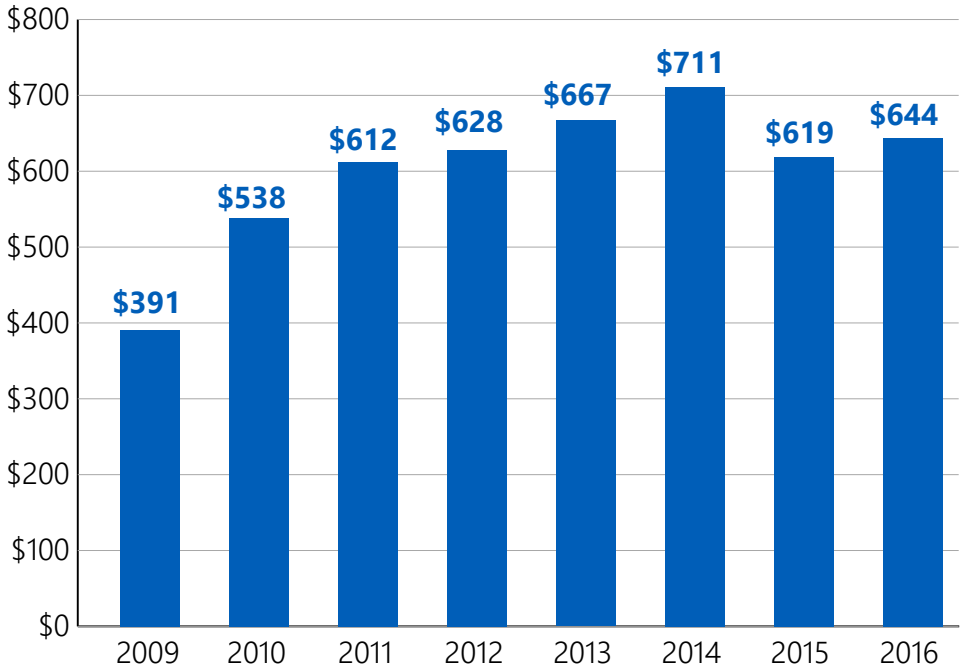
20 *Contemporary Biographies in Communications & Media*, p. 110.

21 Kaspersky Lab, "Company Profile," kaspersky.com, 2014, p. 8, https://web.archive.org/web/20250407173445/https://media.kaspersky.com/en/Corporate_Presentation_Q12014.pdf.

22 Patrick Howell O'Neill, "Kaspersky's North American Operations Undergoes Shuffle; Head of PR Leaves Company," CyberScoop, Oct. 11, 2017, https://cyberscoop.com/kaspersky-north-america-jennifer-wood/.

23 See, for example, Terry Macalister and Tom Parfitt, "$20bn Gas Project Seized by Russia," *The Guardian*, Dec. 12, 2006, https://www.theguardian.com/world/2006/dec/12/business.oil; Clifford J. Levy, "In Hard Times, Russia Tries to Reclaim Industries," *New York Times*, Dec. 7, 2008, https://www.nytimes.com/2008/12/08/world/europe/08kremlin.html; "Government Takes Russia's NTV," ABC News, Apr. 14, 2001, https://abcnews.go.com/International/story?id=81235&page=1.

Figure 1. Kaspersky annual worldwide revenue (2009–2016, in USD millions)



Source: Adapted from Dean Takahashi, "Private Equity Firm General Atlantic Takes $200M Stake in Security Software Vendor Kaspersky Lab," Venture Beat, Jan. 19, 2011, https://venturebeat.com/security/private-equity-firm-general-atlantic-takes-200m-stake-in-security-software-vendor-kaspersky-lab/; Mike Lennon, "Kaspersky Lab 2011 Revenue Tops $612 Million, but No IPO in Sight," securityweek.com, Feb. 10, 2012, https://www.securityweek.com/kaspersky-lab-2011-revenue-tops-612-million-no-ipo-sight/; Kaspersky Lab, "Company Profile," kaspersky.com, 2014, https://media.kaspersky.com/en/Corporate_Presentation_Q12014.pdf; Kaspersky, "Report*: In 2014 Kaspersky Lab Grew Faster Than the Market," Kaspersky.com, Jan. 8, 2016, https://www.kaspersky.com/about/press-releases/report-in-2014-kaspersky-lab-grew-faster-than-the-market; Sarah Kuranda, "Kaspersky Removed from GSA Schedule, Limiting Federal Sales for Its Security Software," crn.com, July 12, 2017, https://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software; "Kaspersky Lab Reports Growth Despite U.S. Government Ban," Radio Free Europe/Radio Liberty, Jan. 20, 2018, https://www.rferl.org/a/kaspersky-reports-8-percent-revenue-growth-despite-us-government-ban-software-/28986290.html.

relations with both the FSB cybersecurity department and the Moscow police department. They know us. They know us as people who support them when they need it."[24] In response to the story, Eugene Kaspersky vehemently denied the existence of any suspicious relationship. He wrote on his blog that the facts were inaccurately reported and that "all three of the world's leading security companies—Symantec, McAfee/Intel, and Kaspersky Lab—work with law enforcement bodies worldwide to help fight cyber-crime" and that "we provide EXPERTISE. Nothing more."[25]

[24] Noah Schachtman, "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals," *WIRED*, July 23, 2012, https://www.wired.com/2012/07/ff-kaspersky/.

[25] Eugene Kaspersky, "What Wired Is Not Telling You—A Response to Noah Shachtman's Article in Wired Magazine," Eugene.kaspersky.com, July 25, 2012, https://web.archive.org/web/20120726135749/https://eugene.kaspersky.com/2012/07/25/what-wired-is-not-telling-you-a-response-to-noah-shachtmans-article-in-wired-magazine/.

Western skepticism of Kaspersky did not end with that story. Bloomberg reported in March 2015 that since 2012, "High-level managers [at Kaspersky] ha[d] left or been fired, their jobs often filled by people with closer ties to Russia's military or intelligence services." The article further claimed that Kaspersky's chief legal officer had since 2013 managed a team of 10 specialists who "provide technical support to the FSB and other Russian agencies" that can "access data directly from any of the company's systems."[26] A few months later, Ukraine sanctioned Kaspersky and banned the use of its software in September 2015, prompting Kaspersky to close its regional office in the country.[27] However, Kaspersky said the company would continue selling products in Ukraine via distribution channels.[28]

In July 2017, Bloomberg wrote about previously unreported emails from Eugene Kaspersky to senior Kaspersky staff in October 2009, which described a secret project initiated the year prior "per a big request on the Lubyanka side."[29] (Lubyanka is the headquarters of the FSB—and, formerly, the KGB.) In addition to protecting the agency from distributed denial of service attacks designed to knock computers offline by flooding them with traffic, Kaspersky said it would assist the FSB with "active countermeasures," which the article claimed was likely a euphemism for hacking back into the systems of people hacking into the FSB.[30]

Kaspersky may have engaged in this activity for a variety of reasons. As Eugene Kaspersky expressed, all kinds of companies in all kinds of countries work with law enforcement in their borders, so a Russian cyber firm working with a Russian security agency would not be unusual.[31] Perhaps Kaspersky was allowed to continue its global business operations in exchange for quietly setting up operational support to the government (a quid pro quo). Perhaps Kaspersky heard the FSB was looking for support, and Kaspersky wanted a new client. Or perhaps Kaspersky pitched the FSB on its capabilities, and the agency saw value and executed a contract. There are many possible overlapping explanations.

Kaspersky's credibility in America and the West received another blow in 2017. The US Department of Homeland Security (DHS) issued a binding operational directive in September 2017 ordering federal agencies to stop using 10 Kaspersky products and services: Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security, Kaspersky Small Office Security, Kaspersky Anti Targeted Attack, Kaspersky Endpoint Security, Kaspersky Cloud Security (Enterprise), Kaspersky Cybersecurity Services, Kaspersky Private Security Network, and Kaspersky Embedded Systems Security. The directive exempted Kaspersky Threat Intelligence and Kaspersky Security Training, ostensibly because American security analysts may still wish to see what

---

[26] Carol Matlack, Michael A. Riley, and Jordan Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies," Bloomberg, Mar. 19, 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies.

[27] Decree of the President of Ukraine No. 549, Sept. 16, 2025, https://www.president.gov.ua/documents/5492015-19437; "Ukraine Bans Russian Anti-Virus Kaspersky Lab Software—Cabinet of Ministers," TASS, Sept. 25, 2015, https://tass.com/economy/823636; "Kaspersky Lab Closes Regional Office in Ukraine," TASS, Dec. 14, 2016, https://tass.com/economy/919394.

[28] "Kaspersky Lab Closes Regional Office in Ukraine."

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

[30] Robertson and Riley, "Kaspersky Lab Has Been Working with Russian Intelligence."

[31] Of course, providing cyber support to Russian security agencies and German ones during the period in question is not equivalent—the former country is a dictatorship and the latter a rule-of-law democracy. The former's security agencies engage in repression, rights abuses, and aggressive intelligence operations abroad, and the latter's have relative checks and balances.

Kaspersky puts into its feeds.[32] The government's directive did not provide any public reasoning for the ban.

The *Wall Street Journal* reported in October 2017 that Russian government hackers had previously "stole[n] details of how the US perpetrates foreign computer networks and defends against cyberattacks" from a contractor "after identifying the files through the contractor's use of a popular antivirus software" made by Kaspersky.[33] Right after that report, the *New York Times* reported that Israeli intelligence officers "who had hacked into Kaspersky's own network" had alerted the United States that they had "looked on in real time as Russian government hackers searched computers around the world for the code names of American intelligence programs" using Kaspersky antivirus software.[34] The *Wall Street Journal* then quoted a former US official as saying that "there is no way, based on what the software was doing, that Kaspersky couldn't have known about this."[35]

Kaspersky again refuted the reporting, but it did not regain its ability to contract with the US government. A judge overruled Kaspersky's lawsuit against the DHS ban in 2018 and kept the prohibition in place.[36] Even so, the company kept expanding its global business operations, including in the West. In July 2016, for instance, it launched a partnership with the Dutch National Police, Europol, and McAfee to educate people about ransomware and to help them recover data without paying ransoms.[37] It regularly cooperated with police forces in European countries, such as Belgium, to assist with cybercrime investigations and incident mitigations well after the DHS ban was issued.[38] And Kaspersky's revenue, as captured in Figure 2, kept increasing until it reached $752 million globally in 2021.

The firm's shift from being a trusted major cybersecurity vendor to one that is reportedly tied to the Russian state provides insights into Russia's private sector cyber ecosystem. Essentially, a private company was created to competitively offer services that others in the country were not offering, and its innovation made it a competitor not just in Russia but around the world. Despite its entrepreneurial origins, the company remained susceptible to the influence of the Russian security services. Kaspersky may have approached the Russian government, or the Russian government may have approached Kaspersky—the reporting is unclear on the order. Either way, the stories underscore that companies in Russia may choose to work with the state of their

---

[32] "Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses," Department of Homeland Security, 82 *FR* 43782, Sept. 19, 2017, https://www.federalregister.gov/documents/2017/09/19/2017-19838/national-protection-and-programs-directorate-notification-of-issuance-of-binding-operational.

[33] Gordon Lubold and Shane Harris, "Russian Hackers Stole NSA Data on US Cyber Defense," *Wall Street Journal*, Oct. 5, 2017, https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

[34] Nicole Perlroth and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for US Secrets," *New York Times*, Oct. 10, 2017, https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

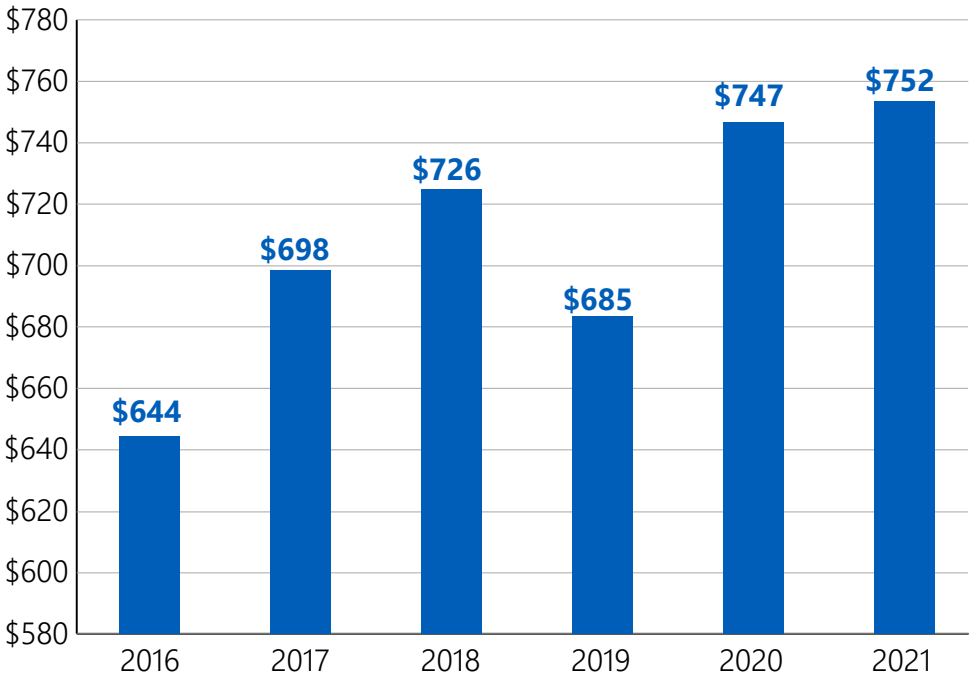
[35] Shane Harris and Gordon Lubold, "Russia Has Turned Kaspersky Software into Tool for Spying," *Wall Street Journal*, Oct. 11, 2017, https://www.wsj.com/articles/russian-hackers-scanned-networks-world-wide-for-secret-u-s-data-1507743874.

[36] Derek B. Johnson, "Judge Upholds Government Ban on Kaspersky Products," Nextgov/FCW, May 30, 2018, https://www.nextgov.com/cybersecurity/2018/05/judge-upholds-government-ban-on-kaspersky-products/196295/.

[37] Kaspersky, "No More Ransom: Law Enforcement and IT Companies Join Forces to Fight Ransomware," Kaspersky.com, July 25, 2016, https://web.archive.org/web/20241008112716/https://www.kaspersky.com/about/press-releases/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware.

[38] Europol, "No More Ransom Update: Belgian Federal Police Releases Free Decryption Keys for the Cryakl Ransomware," Europol.europa.eu, Feb. 9, 2018, https://www.europol.europa.eu/media-press/newsroom/news/no-more-ransom-update-belgian-federal-police-releases-free-decryption-keys-for-cryakl-ransomware.

Figure 2. Kaspersky annual worldwide revenue (2016–2021, in USD millions)



Source: Adapted from Kaspersky, "Kaspersky Lab Announces 4% Revenue Growth to $726 Million in 2018," Kaspersky.com, Feb. 19, 2019, https://www.kaspersky.com/about/press-releases/kaspersky-lab-announces-4-percent-revenue-growth-to-726-million-dollars-in-2018; Kaspersky, "Kaspersky Reports 2019 Financial Results," Kaspersky.com, July 24, 2020, https://www.kaspersky.com/about/press-releases/kaspersky-reports-2019-financial-results; Kaspersky, "Kaspersky Reports Financial Results with Stable Business Growth in 2020," Kaspersky.com, Apr. 19, 2021, https://www.kaspersky.com/about/press-releases/kaspersky-reports-financial-results-with-stable-business-growth-in-2020; Kaspersky, "Kaspersky Reports 2021 Financial Results," Kaspersky.com, June 10, 2022, https://www.kaspersky.com/about/press-releases/kaspersky-reports-2021-financial-results.

own volition or may feel compelled to do so, even if they are not state controlled.

Governments and companies around the world have reacted differently to the potential for Russian government contracting or coercion. The US government's sentiments toward Kaspersky did not prompt other government bodies (such as those in Europe) or all of its commercial clients (such as those in Europe and Latin America) to immediately stop working with the company. European government bodies and companies may not have perceived the same set of risks as the United States did, perhaps because they perceived a lower level of exposure to potential Kaspersky-enabled espionage or perhaps because they did not receive the same threat intelligence from Israel that the US government reportedly received. It is likewise possible that European policy-makers perceived that too many companies were relying on Kaspersky and did not want to force them to shift their systems to a different company. Alternatively, perhaps European countries did see the risk—after all, they well understood Russia's military and intelligence threats and were already imposing waves of sanctions following the illegal 2014 annexation of Crimea—but simply failed to act expediently to mitigate it.

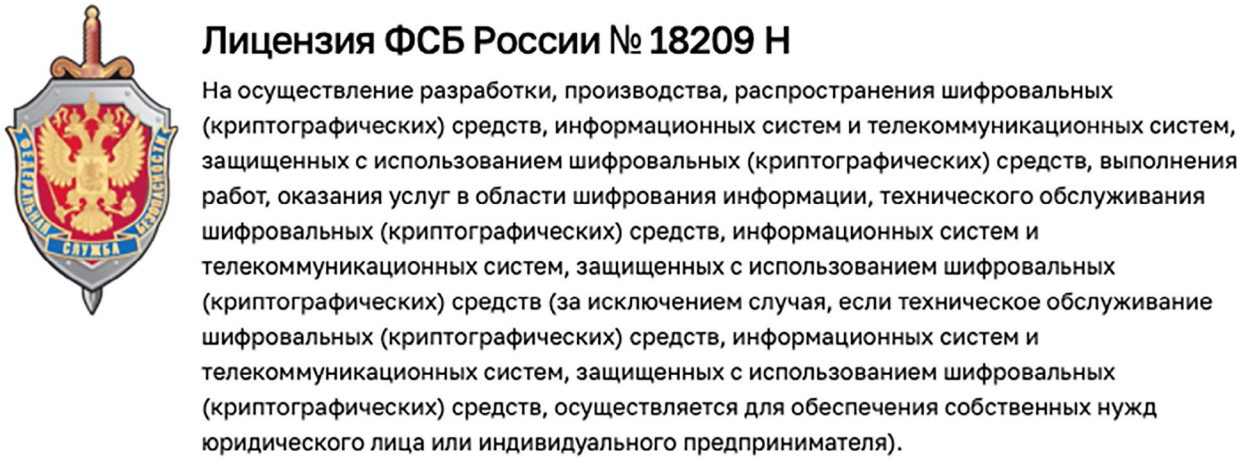
As will be explored in the next section, these differences in perception play out with regard to Russian cyber companies to this day.

Case study #2: Security Code

Security Code is a Russian cybersecurity company that was founded in 1993.[39] Headquartered in Moscow, it provides more than 50,000 organizations with a range of products and services, including network security, virtualization security, endpoint security, mobile security, and electronic signatures.[40] In its Russian-language materials, Security Code has revealed that it provides security-focused services for the Russian state. These services appear to be heavily defensive in nature. Its defensive work spans network security technologies, cryptography, and educational and training programs for public and private Russian universities, including those with military ties.

The company holds several licenses from the FSB, including a No. 18209 N license for the development, production, and distribution of cryptographic systems (see Figure 3); a No. 18210 K license for the development or production of systems designed to protect information designated in Russia as confidential; and a No. 15290 M license, a No. 15289 C license, and a No. 34416 license, all of which are related to the implementation of activities or the provision of services to protect state secrets (ostensibly at higher levels of classification in Russia than confidential, such as at Russia's secret level or above).[41] Security Code also has a license from the MOD (No. 1388) to create information security tools for defense systems and three licenses (Nos. 2457, 0499, and 0829) from the Federal Service for Technical and Export Control, which licenses the export of weapons and dual-use technologies, to create information security tools and develop systems to protect information designated by the state as confidential.[42] In fact, on its English-language and Russian-language home pages, Security Code

Figure 3. Security Code description on website of FSB license no. 18209 N



Source: Security Code, 2025, Securitycode.ru.

[39] Security Code, "About Us," securitycode.net, archived Apr. 9, 2025, https://web.archive.org/web/20250409155741/https://www.securitycode.net/company/.

[40] Security Code, "About Us."

[41] Security Code, "Licenses [« Лицензии »]," Securitycode.ru, archived Aug. 4, 2021, https://web.archive.org/web/20210804210812/https://www.securitycode.ru/company/company-s-licenses/.

[42] Security Code, "Licenses."

notes, under its "five reasons to choose us," that the company has products that are certified by the FSB.[43]

The fact that Security Code holds these licenses, such as the FSB licenses for classified information handling, indicates that it works for Russian government organizations. Security Code also lists many recent government clients on its website, including the following:

- **Federal law enforcement:** FSB, MOD, MVD, Ministry of Emergency Situations, Ministry of Justice, Prosecutor General's Office, Federal Protective Service (FSO), National Guard (Rosgvardia), Federal Penitentiary Service, Investigative Committee, Constitutional Court, and Supreme Court
- **Federal financial authorities:** Ministry of Finance, Federal Treasury, Federal Tax Service, and Central Bank
- **Other public authorities:** Ministry of Foreign Affairs, Pension Fund, Federal Migration Service, Federal Customs Service, Social Insurance Fund, Ministry of Health, Federal Service for the Oversight of Consumer Protection and Welfare (Rospotrebnadzor), Central Election Commission, Federal Compulsory Health Insurance Fund, Federal Tariff Service, Federal Service for the Supervision of Transport, Federal Agency for State Property Management, and Federal Service for Intellectual Property (Rospatent), and Ministry of Digital Development, Communications, and Mass Media
- **State corporations:** Public Joint Stock Company (PJSC) VTB, Russian Railways, Rostec, Gazprom, Rostelecom, Rosneft, Rosatom, Rossetti, Vnesheconombank (VEB), Norilsk Nickel, Joint Stock Company (JSC) Russian Space Systems, Russian Post, Federal State Unitary Enterprise, Sberbank, and Gazprombank[44]

On the same page, the company states that more than 32,000 state and commercial organizations in Russia rely on Security Code to protect devices and networks—suggesting that much, if not all, of its state contracting work focuses on cyberdefense.[45] As described in the previous section, a private cyber firm supporting government clients is not unique to Russia. Yet it is important for Western observers to know that Security Code is supporting Russian security agencies such as the FSB, MOD, and FSO, as well as state corporations such as Rostec, Gazprom, and Rostelecom, so they can better understand the Russian cybersecurity landscape and how Russia is defending against Ukrainian and other operations in wartime.

In addition to cyberdefensive support, the company provides educational services and helps state institutions develop cybersecurity training programs. Several of its dozens of higher educational partners in Russia are public, including the National Research Nuclear University (MEPhI), the National Research University (MPEI), ITMO University, the St. Petersburg State University of Telecommunications, and the Financial University under the Government of the Russian Federation.[46] Some of these universities feed into Russian government military objectives;

---

[43] Security Code, "About Us"; Security Code, "About the Company [« О компании, »]," Securitycode.ru, archived June 19, 2021, https://web.archive.org/web/20210619151914/https://www.securitycode.ru/company/.

[44] Security Code, "Clients [« Клиенты »]," Securitycode.ru, archived Aug. 4, 2021, https://web.archive.org/web/20210804223837/https://www.securitycode.ru/clients/.

[45] Security Code, "Clients."

[46] Security Code, "Education [« Обучение »]," Securitycode.ru, archived Sept. 16, 2021, https://web.archive.org/web/20210916230243/https://www.securitycode.ru/company/training/.

the ITMO, for example, has launched educational programs to train Russians in drone technology, the knowledge of which is in high demand in the Russian armed forces and could be applied directly on the battlefield in Ukraine.[47]

Security Code works with other public universities that have more direct security or military involvement—meaning that cybersecurity training programs at those universities are feeding directly into Russian government military, intelligence, or security activities. MEPhI's Dimitrovgrad Engineering and Technical Institute, for example, was stood up in 2011 out of a Defense Ministry directive to produce experts in nuclear technologies and medicine and in related information technology and computer science fields.[48] MPEI runs a military training center, stood up in 2017, to help train reserve officers and reserve sergeants to enter the Russian air and space forces. Of note, their training includes how to appropriately command automated control systems and communication points.[49] In addition, graduates of MPEI have previously been invited to join the MOD's 4th Central Research Institute to research military scientific support for R&D and tactical and technical protection for military systems against unauthorized use.[50] Even some of Security Code's private university partners, such as the Moscow Technical University of Communications and Informatics, now conduct military training on radios, satellite communications, and related topics at the MOD's behest.[51]

Security Code works with other public universities that have more direct security or military involvement—meaning that cybersecurity training programs at those universities are feeding directly into Russian government military, intelligence, or security activities.

[47] "'Aerokitties' Fly in Swarms. How Higher Education Programs in Drone Technology Service Military Objectives," T-invariant.org, Feb. 20, 2025, https://t-invariant.org/2025/02/aerokitties-fly-in-swarms-how-higher-education-programs-in-drone-technology-serve-military-objectives/; *Artificial Intelligence in Russia: Issue 8, August 14, 2020*, CNA, Aug. 2020, p. 10, https://apps.dtic.mil/sti/trecms/pdf/AD1120632.pdf.

[48] "Dimitrovgrad Engineering and Technical Institute—Branch of Federal Autonomous Higher Vocational Educational Institution 'National Research Nuclear University MEPhI,'" Cluster-dgrad.ru, archived Apr. 9, 2025, https://web.archive.org/web/20250409170129/https://cluster-dgrad.ru/en/members-project/35-national-research-nuclear-university-mifi.

[49] Military Study Center [Военный учебный центр (ВУЦ)], Vuc.mpei.ru, archived Apr. 9, 2025, https://web.archive.org/web/20250409171215/https://vuc.mpei.ru/Pages/default.aspx.

[50] Federal State Budgetary Institution "4th Central Research Institute" of the Ministry of Defense of the Russian Federation [« ФГБУ "4 Центральный научно-исследовательский институт" Министерства обороны Российской Федерации »], Mpei.ru, Jan. 4, 2019, https://web.archive.org/web/20250409171233/https://mpei.ru/Structure/uchchast/educadmin/deptf/Lists/jobList/NewDispForm.aspx?ID=460&RootFolder=%2FStructure%2Fuchchast%2Feducadmin%2Fdeptf%2FLists%2FjobList&Source=https%3A%2F%2Fmpei%2Eru%2FStructure%2Fuchchast%2Feducadmin%2Fdeptf%2FPages%2Fjob%2Easpx%3Fp%3D5.

[51] "The Ministry of Defense Will Consider the Idea of Creating Military Training Centers at the Universities of the Ministry of Digital Development [« Минобороны рассмотрит идею создания военно-учебных центров в вузах Минцифры »]," TASS, Dec. 26, 2023, https://tass.ru/obschestvo/19629995; Military Study Center [Военный учебный центр (ВУЦ)], Sut.ru, archived Apr. 9, 2025, https://web.archive.org/web/20250409173833/https://www.sut.ru/university/structure/vuc; Military Study Center at St. Petersburg State Communications University [Военный Учебный Центр СПБГУТ], Mil.spbsut.ru, archived Apr. 9, 2025, https://web.archive.org/web/20250403120156/https://mil.spbsut.ru/.

Again, this kind of public-private phenomenon is not unique to Russia. For instance, private cybersecurity companies throughout the West commonly team up with public universities to help educate future scholars and practitioners on cybersecurity topics such as encryption, vulnerability research, and data breach response. In addition, the US government routinely stresses the importance of public-private partnerships for cybersecurity.[52]

However, these public-private relationships in Russia are still concerning for the West. Some of the individuals trained in these programs could join the Russian military or intelligence services—an outcome that some of the university pipelines desire. For example, the FSB and its predecessors have been known to recruit cyber personnel from MEPhI.[53] Some of the individuals might go into the private sector and then provide similar offensive, defensive, or other support to the state. In general, the programs build up the cyber talent ecosystem in Russia. Years ago, the global technology community might have seen the most benefit from this buildup of talent, but nationalistic, regime-directed forces have made the Russian government the main beneficiary.

Security Code illustrates that private sector companies are providing cyber support for the Russian government. That support can be defensive, rather than focused on activities related to intelligence operations.

Security Code illustrates that private sector companies are providing cyber support for the Russian government. That support can be defensive, rather than focused on activities related to intelligence operations. That support can also involve defending organizations that present security concerns to the West and the United States, such as helping the FSB and MOD mitigate cyber intrusions and prevent unintended data leaks.[54] Finally, private sector cyber support can include working with public and private universities to train future talent and increase Russia's national cyber capacity.

[52] For instance, the last two administrations' cyber strategies both emphasized this issue. See White House, *National Cybersecurity Strategy*, Mar. 2023, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; White House, *National Cyber Strategy of the United States of America*, Sept. 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[53] Andrei Soldatov and Irina Borogan, *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*, Center for European Policy Analysis, Sept. 2022, pp. 7, 9, 14, https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

[54] Although there is little information available about Security Code's exact activities for these agencies, it began helping the MOD in 2011, for example, by securing virtualized infrastructure (e.g., infrastructure run by VMWare) and making its trusted boot unit "Sobol" available to MOD-subordinate organizations. These are defensive functions.

Case study #3: Positive Technologies

Positive Technologies was founded in 2002 after two security entrepreneurs built a security scanner called XSpider in 1998.[55] It was the first cyber firm publicly available on the Moscow Exchange.[56] With offices in Moscow, Saint Petersburg, Nizhny Novgorod, Novosibirsk, Samara, and Tomsk, as well as in Dubai, United Arab Emirates, the company currently provides cybersecurity services and technologies to more than 4,000 organizations around the world.[57] Those services and technologies span perimeter and network threat detection, sandboxes and virtual environments, vulnerability management, infrastructure threat detection, application security testing, incident response, endpoint protection, firewalls, email security, threat intelligence, and industrial cybersecurity.[58] Unlike Security Code, however, it apparently supports Russian intelligence agencies with offensive operations and intelligence recruitment through multiple lines of effort.

The clients listed on its website span the energy, financial, state, telecommunications, oil and gas, and other sectors. They include Russian energy companies, such as Rosenergoatom Concern (the Russian nuclear power station subsidiary of state-owned nuclear firm Rosatom); financial institutions, such as Alfa-Bank; and government agencies, such as the MVD, the Ministry of Foreign Affairs, the MOD, the FSB, the government of Moscow, the Federal Customs Service, and Roskomnadzor (the media and internet regulator and censor).[59] Positive Technologies also has clients among government agencies in the broader post-Soviet space, such as the Ministry of Finance in Kazakhstan.[60] The company's work for the MOD dates back to 2004, and the timeline of its work for the other clients (such as the FSB or Roskomnadzor) is unclear.[61]

Positive Technologies was founded in 2002 after two security entrepreneurs built a security scanner called XSpider in 1998. It was the first cyber firm publicly available on the Moscow Exchange.

In April 2021, the US government sanctioned Positive Technologies for supporting Russian government clients, including the FSB.[62] The Treasury Department justified the sanctions in a statement: "Positive Technologies provides computer network security

[55] Positive Technologies, "About Us," Ptsecurity.com, archived Apr. 8, 2025, https://web.archive.org/web/20250408173347/https://global.ptsecurity.com/about.

[56] Positive Technologies, "About Us."

[57] Positive Technologies, "Contacts," Ptsecurity.com, archived Apr. 21, 2025, https://web.archive.org/web/20250421163932/https://global.ptsecurity.com/about/contacts; Positive Technologies, "About Us."

[58] Positive Technologies, "About Us."

[59] "Rosenergoatom Concern JSC: Overview," Globaldata.com, accessed Apr. 21, 2025, https://www.globaldata.com/company-profile/rosenergoatom-concern-jsc/; Positive Technologies, "Our Clients [«Наши клиенты»]," Ptsecurity.com, archived Apr. 3, 2025, https://web.archive.org/web/20250403060911/https://www.ptsecurity.com/ru-ru/about/clients/#gos-uchrezhdeniya.

[60] Positive Technologies, "Our Clients."

[61] Positive Technologies, "About Us."

[62] US Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority."

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."[63] This statement provides three pieces of information: the company's work with the FSB was of concern to the US government, Positive Technologies was running conventions that were leveraged for intelligence service recruitment, and the company was potentially involved through said convention with the GRU, which was not—and is still not as of this report—listed on its website as a client.

Positive Technologies had previously shown *Forbes* that it could bypass encryption mechanisms in Signaling System No. 7 (SS7), the international telecommunications protocol, to receive all messages intended for a target device.[64] *MIT Technology Review* then reported in April 2021—the same day that the sanctioning was announced—that "privately, the US has concluded that Positive [Technologies] did not just discover and publicize flaws in the system, but also developed offensive hacking capabilities to exploit security holes that were then used by Russian intelligence in cyber campaigns."[65] It continued, "Former US officials say there is a tight working relationship with the Russian intelligence agency FSB that includes exploit discovery, malware development, and even reverse engineering of cyber capabilities used by Western nations like the United States against Russia itself."[66] One former American intelligence official, quoted anonymously, called the kind of relationship that Positive Technologies has with the state "complex" and "abusive," saying—as the publication paraphrased it—that "the pay is relatively low, the demands are one-sided, the power dynamic is skewed, and the implicit threat for non-cooperation can loom large."[67]

Positive Technologies builds and offers defense-oriented services for clients that ostensibly include government clients. For instance, it launched a series of corporate centers in 2017 in partnership with another Russian cyber firm (Solar Security) to support GosSOPKA, the government's national cyber threat information-sharing and detection system.[68] In addition, the media has reported that Positive Technologies turns vulnerabilities it discovers into exploits for the FSB and reverse engineers Western cyber capabilities, indicating that it actively supports offensive operations.

In addition, Positive Technologies hosts a flagship annual conference called Positive Hack Days, which has been dubbed Russia's DEF CON or Black Hat (referring to the major US hacker conferences). The event is both the country's largest cybersecurity conference and the country's largest capture-the-flag competition between hackers. The US government has stated that the conference is a recruiting zone for

63 US Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority."

64 Thomas Brewster, "Watch as Hackers Hijack WhatsApp Accounts via Critical Telecom Flaws," *Forbes*, June 1, 2016, https://www.forbes.com/sites/thomasbrewster/2016/06/01/whatsapp-telegram-ss7-hacks/?sh=3e2c9546178b.

65 Patrick Howell O'Neill, "The $1 Billion Russian Cyber Company That the US Says Hacks for Moscow," *MIT Technology Review*, Apr. 15, 2021, https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/.

66 O'Neill, "The $1 Billion Russian Cyber Company That the US Says Hacks for Moscow."

67 O'Neill, "The $1 Billion Russian Cyber Company That the US Says Hacks for Moscow."

68 "Solar Security and Positive Technologies to Create Cybersecurity Centers [« Solar Security и Positive Technologies займутся созданием центров кибербезопасности »]," Astera.ru, Nov. 20, 2017, https://astera.ru/news/solar-security-i-positive-technologies-zajmutsya-sozdaniem-tsentrov-k/. For more on GosSOPKA, see the excellent recent discussion in Luke Rodeheffer, "Russia Ramps Up Cybersecurity Systems," *Eurasia Daily Monitor* 22, no. 15 (Feb. 6, 2025), https://jamestown.org/program/russia-ramps-up-cybersecurity-systems/.

the Russian security services.[69] According to the *Daily Beast*, GRU and FSB officers, including an individual in GRU Unit 74455 (popularly known as Sandworm), have attended the event while participating hackers competed in exercises such as shutting down a mock city's electrical grid.[70] Recruiting at a cyber conference is not unusual; many countries recruit software developers for their security services from conferences around the world. However, in this case, Russia would be recruiting software developers to assist with offensive functions.

Positive Technologies and Kaspersky have similarities and differences. Both are private companies that have been reportedly involved in supporting Russian offensive cyber activities. They both can draw on significant talent and technology to support those efforts, and they publicly advertise their services as defensive. Yet Kaspersky is a globally known cybersecurity company, whereas Positive Technologies was not well known outside of Russia before the US sanctioned it in 2021. Unlike Kaspersky, Positive Technologies does not have a flagship, globally integrated antivirus product that could give it immediate system access to computers around the world, nor does it have the kinds of business relationships that Kaspersky has built with thousands of firms worldwide.

Nonetheless, Kaspersky and Positive Technologies have one core similarity: their hidden support for the Russian state raises critical supply chain security and due diligence questions for other private companies. For years, Positive Technologies was part of Microsoft's Active Protections Program, through which Microsoft disseminates early information about vulnerabilities.[71] Based on news reports, if Positive Technologies were to access such a feed, it would potentially be able to pass information in real time to the FSB and help it exploit the flaws before they were disclosed and addressed. Hence, when Positive Technologies was sanctioned, Microsoft said it would remove the company from the program.[72] This example demonstrates that many private sector offensive relationships are covert, and Western companies may have to suddenly pivot their supply chains and trust calculi when such contractors become known.

Positive Technologies' reported offensive support for the FSB prompts further analytical questions about its engagements with other state clients. It is plausible that Positive Technologies works with the FSB on vulnerability discovery and exploit development, with the FSB and GRU on intelligence recruitment, and with other clients on entirely defensive matters, such as responding to breaches and detecting systems brought online with default passwords. It is also plausible that Positive Technologies—whether by choice, compliance with law or coercion, or some combination—does not contain its offensive

---

[69] The Treasury sanction announcement does not refer to Positive Hack Days specifically, but it is a reasonable inference given that it is Positive Technologies' flagship annual event and that other reporting (cited later in the paper) noted that GRU and FSB officers attended the event.

[70] US Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," Justice.gov, Oct. 19, 2020, https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and; Kevin Pulsen, "This Hacker Party Is Ground Zero for Russia's Cyberspies," *Daily Beast*, Aug. 3, 2018, https://www.thedailybeast.com/this-hacker-party-is-ground-zero-for-russias-cyberspies-3/.

[71] Frank Bajak and Matt O'Brien, "Sanctioned Russian IT Firm Was Partner with Microsoft, IBM," Associated Press, Apr. 15, 2021, https://apnews.com/article/business-europe-hacking-russia-dd8c331ff30d366ea4f5d828e788c307; Kim Zetter, "Sanctioned Firm Accused of Helping Russian Intelligence Was Part of Microsoft's Early Vuln Access Program—MAPP," Zero Day, Apr. 16, 2021, https://www.zetter-zeroday.com/sanctioned-firm-accused-of-helping/.

[72] Zetter, "Sanctioned Firm Accused of Helping Russian Intelligence Was Part of Microsoft's Early Vuln Access Program—MAPP."

support to the FSB. For instance, one of its clients is the MVD, which runs the police forces around the country that are responsible for day-to-day order.[73] In this case, "order" includes suppressing dissent. Another of its clients is Roskomnadzor, which had primarily regulated and censored the media since its 2008 founding but has taken on a quasi-intelligence role within the country since roughly 2020, helping to track and identify dissidents.[74] Both organizations could be interested in hacking capabilities.

More broadly, Positive Technologies' recruitment activities demonstrate the entrepreneurialism all throughout the Russian cyber web, including from government agencies. For example, the MOD has mimicked the FSB's conference recruitment tactics by developing its own cybersecurity events with companies and hackers.[75] Clearly, the MOD saw the benefits of such an initiative and sought to replicate it.

[73] See, for example, Andrew S. Bowen, *Russian Law Enforcement and Internal Security Agencies*, IF11647 Congressional Research Service, Sept. 2020, https://www.congress.gov/crs-product/IF11647; Mark Galeotti, *The Law Enforcement Agencies: Russian Domestic Security and International Implications*, George C. Marshall European Center for Security Studies, Feb. 2020, https://www.marshallcenter.org/en/publications/security-insights/law-enforcement-agencies-russian-domestic-security-and-international-implications-0; Mariya Y. Omelicheva, *Repression Trap: The Mechanism of Escalating State Violence in Russia*, Center for Strategic & International Studies, July 2021, https://www.csis.org/analysis/repression-trap-mechanism-escalating-state-violence-russia.

[74] Justin Sherman, "Russia's Internet Censor Is Also a Surveillance Machine," Council on Foreign Relations, Sept. 28, 2022, https://www.cfr.org/blog/russias-internet-censor-also-surveillance-machine; Daniil Belovodyev, Anton Bayev, and Systema, "Inside the Obscure Russian Agency That Censors the Internet: An RFE/RL Investigation," Radio Free Europe/Radio Liberty, Feb. 9, 2023, https://www.rferl.org/a/russia-agency-internet-censorship/32262102.html.

[75] Soldatov and Borogan, *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*, p. 17.

Grow, Adapt, Expand: Russian Cyber Firms After 2022

Since the full-scale invasion of Ukraine, Russian cyber firms have lost many contracts and engagements in the United States and the West. They have been subject to newfound sanctions and export controls. In addition, Russian cyber firms are having to use Russian or Chinese products rather than Western ones because of invigorated enforcement of domestic software and hardware rules. Even so, cybersecurity companies have "shadow" installed software they are not legally supposed to have in order to keep systems and business operations running. Cybersecurity companies have also leaned more into security rhetoric to land state contracts, pivoted to greater relationship-building with Asian countries such as India and China, and leaned into the heightened demand for cyber services in Russia during the war.[76] As detailed in this section, many of them have significantly increased their profits. Far more than some other areas of the economy, Russia's private sector cybersecurity industry has proven relatively resilient since February 2022.

In particular, many Russian cybersecurity companies have successfully expanded their business operations globally. Several have expanded into Latin America, Africa, the Middle East, and the Asia-Pacific. Reasons for this push include the desire to increase profits, the need to replace profits lost as a result of sanctions and severed business ties, the need to meet market demands for more threat intelligence feeds and innovative cybersecurity offerings, and the desire to reflect the Kremlin's strategic interests in expanding and deepening cyber- and technology-related partnerships across the African continent, in Latin America, and elsewhere. These companies' viability, global technology reach, and ability to support the Russian government in various ways all provoke key questions for analysts, practitioners, and policy-makers in the West.

In particular, many Russian cybersecurity companies have successfully expanded their business operations globally. Several have expanded into Latin America, Africa, the Middle East, and the Asia-Pacific.

Case study #1: Kaspersky

Following the Putin regime's full-scale invasion of Ukraine in February 2022, the United States government did not immediately add Kaspersky to the sanctions list. However, in March 2022, the Federal Communications Commission added Kaspersky to the Covered List, designating it a provider of communications equipment and services

[76] Justin Sherman, "Russia's Largest Hacking Conference: Biggest Hits from Positive Hack Days 2023," Margin Research, Dec. 5, 2023, https://margin.re/2023/12/russias-largest-hacking-conference-biggest-hits-from-positive-hack-days-2023-2/.

that pose a threat to national security.[77] In June 2024, the Commerce Department's Bureau of Industry and Security (BIS) exercised an authority for the first time. Under the Information and Communications Technology and Services Supply Chain program (first stood up by President Donald Trump in his first term), it banned several Kaspersky products and services in the United States.[78] Unlike DHS's binding directive in 2017, which was focused on only government systems, the BIS order restricted several of Kaspersky's business elements in the United States.

That same month, the Treasury Department sanctioned 12 people in Kaspersky's leadership, including the chief legal officer, the director of future technologies, and the managing director for Russia and the Commonwealth of Independent States countries.[79] The Treasury Department's announcement seemed to align with the allegations the media had printed about Kaspersky: Treasury sanctioned Kaspersky's chief legal officer, for example, which was exactly the role that Bloomberg reported was in charge of a small company team providing technical support to the FSB.[80] After the sanction was announced, Kaspersky said it would cease providing antivirus signature and codebase updates beginning September 30, 2024.[81] The company then shut down its one American office in Woburn, Massachusetts, and its office in London, UK (each had about 50 employees).[82]

Other countries began to speak out during this time. Germany's Federal Office for Information Security warned in March 2022 against the use of Kaspersky software because "a Russian IT manufacturer can carry out offensive operations itself, be forced against its will to attack target systems, or be spied on as a victim of a cyber operation without its knowledge or as a tool for attacks against its own customers."[83] Italy started developing rules that same month to block state bodies from using Kaspersky software.[84] In September 2022, Poland, Estonia, Latvia, and Lithuania proposed that the EU ban Kaspersky's use anywhere in the bloc.[85]

Nonetheless, Kaspersky currently has global operations supported by more than 4,000 employees.[86] Based on data from LinkedIn in April

---

77 US Federal Communications Commission, "FCC Expands List of Equipment and Services That Pose Security Threat," FCC.gov, Mar. 25, 2022, https://www.fcc.gov/document/fcc-expands-list-equipment-and-services-pose-security-threat.

78 US Bureau of Industry & Security, "Commerce Department Prohibits Russian Kaspersky Software for US Customers," BIS.gov, June 20, 2024, https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-u.s.-customers.

79 US Department of the Treasury, "Treasury Sanctions Kaspersky Lab Leadership in Response to Continued Cybersecurity Risks," Treasury.gov, June 21, 2024, https://home.treasury.gov/news/press-releases/jy2420.

80 Matlack, Riley, and Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies."

81 Kaspersky, "Kaspersky Statement on Compliance in the US Following ICTS Final Determination," Usa.kaspersky.com, July 18, 2024, https://usa.kaspersky.com/about/press-releases/kaspersky-statement-on-compliance-in-the-us-following-icts-final-determination.

82 Kate Irwin, "Kaspersky Shuts Down US Operations Following Nationwide Ban," *PC Mag*, July 16, 2024, https://www.pcmag.com/news/kaspersky-shutting-down-us-operations-following-nationwide-ban; Lorenzo Franceschi-Bicchierai, "Kaspersky Says It's Closing Down Its UK Office and Laying Off Dozens," *TechCrunch*, Oct. 8, 2024, https://techcrunch.com/2024/10/08/kasperksy-says-its-closing-down-its-uk-office-and-laying-off-dozens/.

83 "Germany Warns Against Russian Anti-Virus Use," BBC, Mar. 15, 2022, https://www.bbc.com/news/technology-60738208.

84 Angelo Amante, "Italy Set to Curb Use of Russian Anti-Virus Software in Public Sector," Reuters, Mar. 17, 2022, https://www.reuters.com/technology/italy-set-curb-use-russian-anti-virus-software-public-sector-2022-03-17/.

85 AJ Vicens, "Can Kaspersky Survive the Ukraine War?," CyberScoop, Sept. 28, 2022, https://cyberscoop.com/kaspersky-ban-europe-russia-government/.

86 Kaspersky, "Company Overview," Kaspersky.com, accessed Mar. 28, 2025, https://web.archive.org/web/20250328105919/https://www.kaspersky.com/about/company.

2025, most of them are physically located in Russia, with several hundred others located across Brazil, India, the United Arab Emirates, and elsewhere.[87] It advertises that it has more than 220,000 corporate clients around the world and boasts 34 offices in more than 30 countries.[88] These offices are located in cities such as São Paulo, Brazil; Mexico City, Mexico; Prague, Czech Republic; Dublin, Ireland; Jerusalem, Israel; Tokyo, Japan; Vorna Valley, South Africa; and Milan, Italy, as well as in Singapore.[89]

Kaspersky has also opened "transparency centers" around the world to combat allegations that organizations using its cybersecurity services are vulnerable to potential exploitation and data exfiltration by the Russian security services. The company opened its first transparency center in Zurich, Switzerland, in 2017 as part of its new Global Transparency Initiative to "further debunk media myths about backdoors or other nonsense," as Kaspersky put it.[90] Since the start of the war, it has used these transparency centers to push further into a range of global markets.

In March 2022, Kaspersky said it started processing and storing malicious and suspicious files from users in Latin America and the Middle East in Zurich, Switzerland, rather than processing the data in Russia.[91] In November 2024, Kaspersky opened its second Latin American center in Bogotá, Colombia (following its 2019 transparency center in São Paulo,

Kaspersky Transparency Center Locations

Bogotá, Colombia
Istanbul, Turkey
Kigali, Rwanda
Kuala Lumpur, Malaysia
Madrid, Spain
Riyadh, Saudi Arabia
Rome, Italy
São Paulo, Brazil
Seoul, South Korea
Singapore
Tokyo, Japan
Utrecht, Netherlands
Zurich, Switzerland

Kaspersky, "Kaspersky Transparency Center," Kaspersky.com, archived Apr. 21, 2025, https://www.kaspersky.com/transparency-center-offices.

[87] According to the company's LinkedIn page, some employees are located within the United States, although it is unclear whether this information reflects changes made following the banning of several Kaspersky products and services in the United States in 2024. See https://www.linkedin.com/company/kaspersky.

[88] Kaspersky, "Company Overview."

[89] Kaspersky LinkedIn page, accessed Apr. 7, 2025; Kaspersky, "Contáctanos," Latam.kaspersky.com, accessed Apr. 7, 2025, https://web.archive.org/web/20250407161533/https://latam.kaspersky.com/about/contact.

[90] Jeffrey Esposito, "A Transparent Move in North America," Usa.kaspersky.com, Dec. 13, 2021, https://usa.kaspersky.com/blog/kaspersky-transparency-center-north-america/25939/.

[91] Kaspersky, "Kaspersky Relocates Cyberthreat-Related Data Processing for Users in Latin America and Middle East to Switzerland and Re-Certifies Its Data Services by TÜV AUSTRIA," Kaspersky.com, Apr. 14, 2022, https://www.kaspersky.com/about/press-releases/kaspersky-relocates-cyberthreat-related-data-processing-for-users-in-latin-america-and-middle-east-to-switzerland-and-re-certifies-its-data-services-by-tuv-austria.

Brazil).[92] Visitors can reportedly visit the sites to get information about the company's supposed internal processes and data management practices, secure development processes, and application security testing. They can also reportedly audit product source code.[93] As of November 2024, 150 Kaspersky Lab employees reportedly work in Latin America, including specialists from Kaspersky's Global Center for Research and Analysis of Threats.[94]

However specious these claims about state independence and transparency may appear to many Western observers, the company's financials indicate they are perceived differently in many parts of the world. Figure 4 shows Kaspersky's annual revenue in 2022, 2023, and 2024, with numbers from 2018 to 2021 included for context. In 2022, despite the full-on war, Kaspersky made almost exactly as much money as it did the year prior, around $752 million. In 2023, its revenue declined about 4.1 percent, to around $721 million. But in 2024, Kaspersky's year-over-year revenue increased about 14 percent, to $822 million—the highest annual revenue in the company's then-27-year history.[95]

This increased revenue challenges a Western assumption that countries in Latin America, the Middle East, and elsewhere would follow along with the United States, much of Europe, and Japan in attempting to limit exposure to Russian cyber products. It shows that there is a demand for not just Kaspersky's threat intelligence feeds—one of the few offerings exempted from the 2024 US ban—but also its defensive software products and services. For example, sales of Kaspersky's Unified Monitoring and Analysis Platform grew 39 percent from 2023 to 2024.[96] Its Anti Targeted Attack Platform (designed to combat advanced persistent threats) saw an 18 percent sales growth in that period.[97] And its new Kaspersky Next product, which merges endpoint detection and response with extended detection and response capabilities, saw a 100 percent increase in sales in 2024.[98]

Many countries around the world are buying Kaspersky products and services even though doing so gives the company deep access to customer systems. Some may be choosing Kaspersky for its expertise and access to threat intelligence; others may be doing so because they distrust American technology firms. Edward Snowden's leaks of classified government intelligence collection programs in 2013 and countless subsequent data privacy abuses by Silicon Valley giants have created a perception that Russian firms offer an alternative, less Washington-dominated set of solutions. Countries that have historically experienced US political interference or whose leaders are supporters of Putin may be especially inclined to work with Russia.

When Kaspersky was first accused in the press of supporting the FSB, its vehement denials appeared rooted in a desire to be viewed as a trusted cybersecurity company—one focused on helping

---

92 "Kaspersky Lab Transparency Center Opens in Colombia [В Колумбии открылся Центр прозрачности «Лаборатории Касперского», d-russia.ru]," Nov. 18, 2024, https://web.archive.org/web/20241118165727/https://d-russia.ru/v-kolumbii-otkrylsja-centr-prozrachnosti-laboratorii-kasperskogo.html.

93 "Kaspersky Lab Transparency Center Opens in Colombia."

94 "Kaspersky Lab Transparency Center Opens in Colombia."

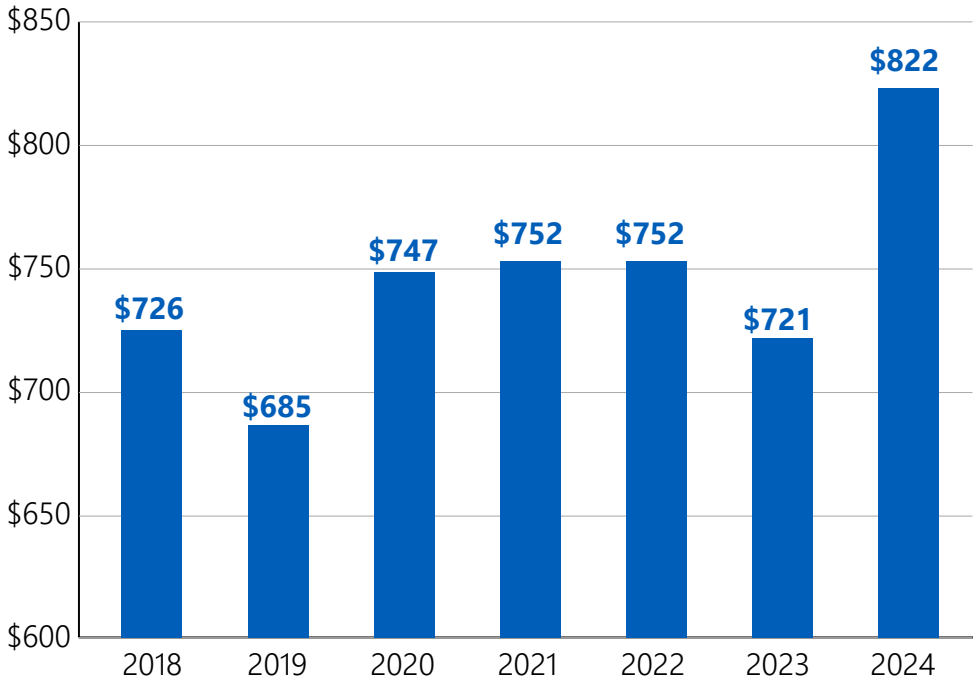
95 Kaspersky, "Kaspersky Reports 2024 Financial Results with Record Revenue," Kaspersky.com, Apr. 9, 2025, https://www.kaspersky.com/about/press-releases/kaspersky-reports-2024-financial-results-with-record-revenue.

96 Kaspersky, "Kaspersky Reports 2024 Financial Results with Record Revenue."

97 Kaspersky, "Kaspersky Reports 2024 Financial Results with Record Revenue."

98 Kaspersky, "Kaspersky Reports 2024 Financial Results with Record Revenue."

Figure 4. Kaspersky annual worldwide revenue (2018–2024, USD millions)



Source: Adapted from Kaspersky, "Kaspersky Lab Announces 4% Revenue Growth to $726 Million in 2018"; Kaspersky, "Kaspersky Reports 2019 Financial Results"; Kaspersky, "Kaspersky Reports Financial Results with Stable Business Growth in 2020"; Kaspersky, "Kaspersky Reports 2021 Financial Results"; Kaspersky, "Kaspersky Reports 2022 Financial Results," Kaspersky.com, June 2, 2023, https://www.kaspersky.com/about/press-releases/kaspersky-reports-2022-financial-results; Kaspersky, "Kaspersky Reports 2023 Financial Results with 11% Business Growth," Kaspersky.com, June 20, 2024, https://www.kaspersky.com/about/press-releases/kaspersky-reports-2023-financial-results-with-11-business-growth; Kaspersky, "Kaspersky Reports 2024 Financial Results with Record Revenue."

people protect themselves. However, in February 2025, it was discovered that Prospero, a notorious Russian "bulletproof" web hosting provider for cybercriminals (meaning one that hides and refuses to disclose its customers, even to governments), had started routing its operations through networks run by Kaspersky.[99] Being linked to a cybercriminal group has subverted its efforts to be viewed as a trusted brand. Whether Kaspersky did so for money, a nudge from the state, or something else completely, it is now engaged in an observable activity it probably would not have performed a decade ago. The second major shift cuts the other way: cybercrime remains a lucrative business in Russia, and Russian cybercriminals now want the protection of a large, proper cybersecurity company.

Case study #2: Security Code

The United States sanctioned Security Code in February 2024, describing it as "a developer of software and hardware used for information security

[99] Brian Krebs, "Notorious Malware, Spam Host 'Prospero' Moves to Kaspersky Lab," Krebsonsecurity.com, Feb. 28, 2025, https://krebsonsecurity.com/2025/02/notorious-malware-spam-host-prospero-moves-to-kaspersky-lab/.

systems," including by the MOD and MVD.[100] Its client list includes more than those two agencies, but its provision of cyberdefensive technologies and services for the military and for internal security forces is still significant. The Ukrainian government had sanctioned Security Code almost a year earlier, in April 2023.[101] Other countries, such as the European Union bloc, have not sanctioned the company, and it has otherwise managed to stay out of the Western press.

Security Code's revenue for 2022, 2023, and 2024 is depicted in Figure 5, with numbers for 2019 to 2021 included for context. In 2021, it earned around $64 million in revenue. In 2022, its revenue increased about 41 percent to around $90 million. In 2023, the company's revenue increased about 24 percent to around $112 million, and in 2024, it increased about another 38 percent to around $154 million. As with Kaspersky, 2024 appears to have been Security Code's highest earning year yet.

Defensive capabilities are in strong demand across Russia, fueled by concern about foreign cyber operations against the country from Ukraine and others. Security Code still lists many government agencies (e.g., the FSB, MOD, FSO, and Ministry of Health) among its clients. The company does not break down its public financials by country, making it difficult to assess its business footprint in Russia compared to other regional countries; however, its commercial director commented in its release of 2024 financials that most of their customers are in charge of "CII," or the Russian government designation of "critical information infrastructure" entities handling information systems, networks, and technologies that are critical to the state's functioning and security.[102] So-called CII entities as defined under Russian law include health care, science, transportation, communications, power, banking, atomic, defense, space, and mining.[103] Because CII is a Russian legal term, the director's comment suggests that most of Security Code's clients are at least headquartered or operating in Russia, which would lend further credence to the theory that wartime defensive demands are driving its growth.

Interestingly, Security Code said that 79 percent of its 2024 revenue came from selling products related to network infrastructure security.[104] These products include its comprehensive network security solution Next-Generation Firewall (NGFW) Continent 4 and some of its hardware and software encryption products.[105] The Russian state may not be able to easily build or acquire such valuable offerings, highlighting its reasons for working with Security Code.

Case study #3: Positive Technologies

Since 2022, Positive Technologies has focused aggressively on international markets and continued to sell its products and services widely, despite multiple public statements and reports about its

[100] US Department of the Treasury, "On Second Anniversary of Russia's Further Invasion of Ukraine and Following the Death of Aleksey Navalny, Treasury Sanctions Hundreds of Targets in Russia and Globally," Treasury.gov, Feb. 23, 2024, https://home.treasury.gov/news/press-releases/jy2117.

[101] "LLC Security Code," Opensanctions.org, accessed Apr. 27, 2025, https://www.opensanctions.org/entities/NK-6sfEe2d9qSQzprVpJysUFH/.

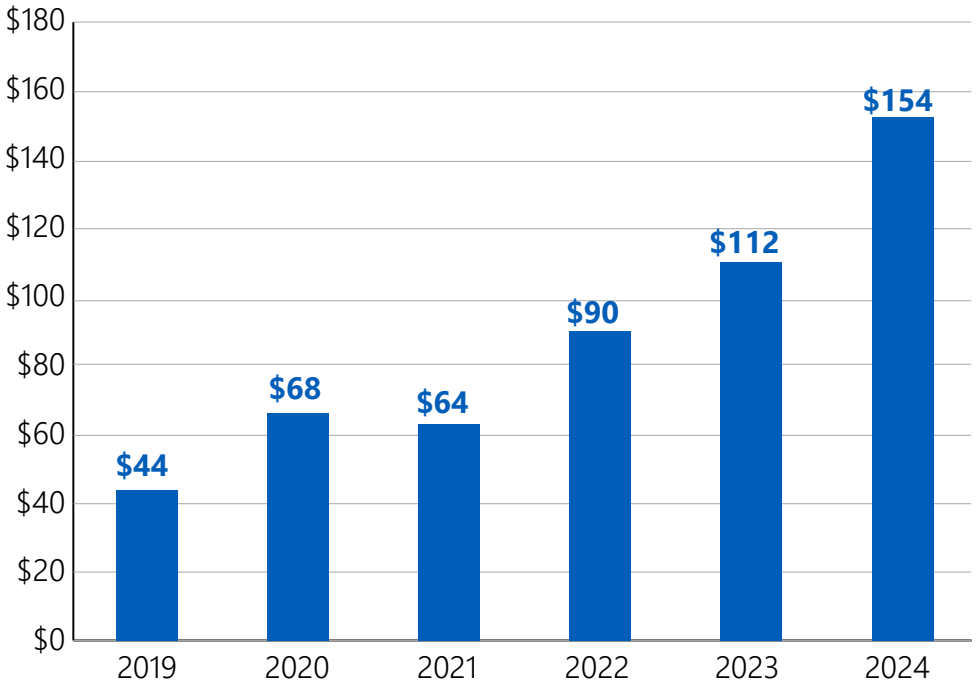
[102] See, for instance, "CII Protection," Satel.ru, accessed Apr. 27, 2025, https://satel.ru/en/integration/cii-protection/.

[103] Russian Federal Law No. 187-FZ, July 26, 2017.

[104] Security Code 2024 financials discussion, pulled from now-unavailable page.

[105] Security Code 2024 financials discussion, pulled from now-unavailable page.

Figure 5. Security Code annual worldwide revenue (2019–2024, in USD millions)



Source: Security Code 2024 financials discussion, pulled from now-unavailable webpage. Sourcing information available from CNA upon request.

direct work for offensive Russian intelligence units. In its marketing, Positive Technologies presents itself as a tool for diversifying an organization's geopolitical risk when it comes to cybersecurity services. It does not suggest that companies forgo American, Chinese, or Israeli cyber providers; rather, it makes the case for adding a Russian vendor.[106]

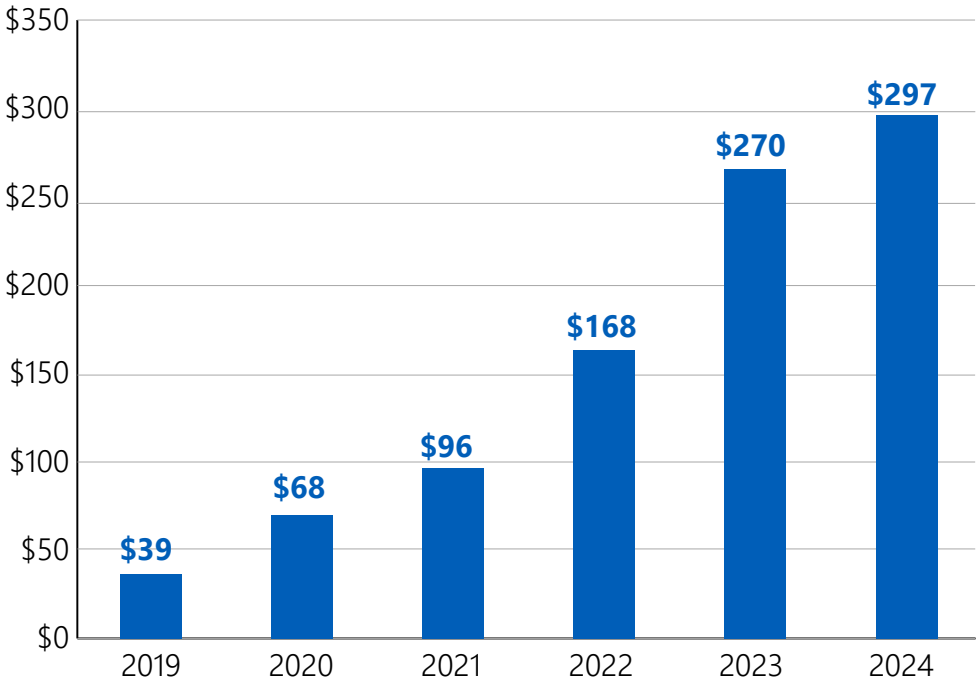
This pitch has evidently paid off. Figure 6 shows Positive Technologies' worldwide annual revenue for 2022, 2023, and 2024, with revenue from 2019 to 2021 included for context.[107] In 2021, the year it was sanctioned by the US government and publicly named as a Russian intelligence contractor, Positive Technologies generated around $96 million in revenue. In 2022, its revenue increased about 75 percent, to around $168 million in revenue—more than tripling its profits.[108] The company attributed part of its success to a substantial increase in the number of product licenses shipped around the world. Then, in 2023, its revenue increased about 61 percent, to around $270 million, and in 2024, its revenue increased about 10 percent, to around $297 million. Its highest revenue year was 2024, despite the war.

[106] Justin Sherman, "Russia's Largest Hacking Conference Reflects Isolated Cyber Ecosystem," Brookings Institution, Jan. 12, 2023, https://www.brookings.edu/articles/russias-largest-hacking-conference-reflects-isolated-cyber-ecosystem/.

[107] "Positive Technologies Financials," Tadviser.com, accessed May 2025, https://tadviser.com/index.php/Article:Positive_Technologies_financials.

[108] "Positive Technologies Financials."

Figure 6. Positive Technologies annual worldwide revenue (2019–2024, in USD millions)



Source: "Positive Technologies Financials."

Positive Technologies' conference attendance has likewise grown significantly. As captured in Figure 7, attendance increased from about 3,800 in 2021 (a recovery from the canceled event in 2020), to about 10,000 in 2022, to a considerable 55,000 in-person attendees in 2023—an increase of 450 percent from the second to the third year.[109] In addition to in-person attendees in 2023, approximately 100,000 people followed the event online, including through Positive Hack Days' new satellite viewing location in Bangkok, Thailand.[110] These numbers indicate significant interest in cybersecurity as a career within Russia, and they suggest that outreach to increase cyber partnerships with other countries—such as in the Asia-Pacific, the Middle East, and North Africa—has been initially successful.

Alongside revenue and conference growth, Positive Technologies has remained focused on talent acquisition within the Russian cyber ecosystem. It even recruited several known talented engineers from Cisco's Moscow office after the full-scale invasion.[111] As of December 2024, Positive Technologies' talent base numbered about 3,160 employees.[112] Looking ahead, members of management have said they view

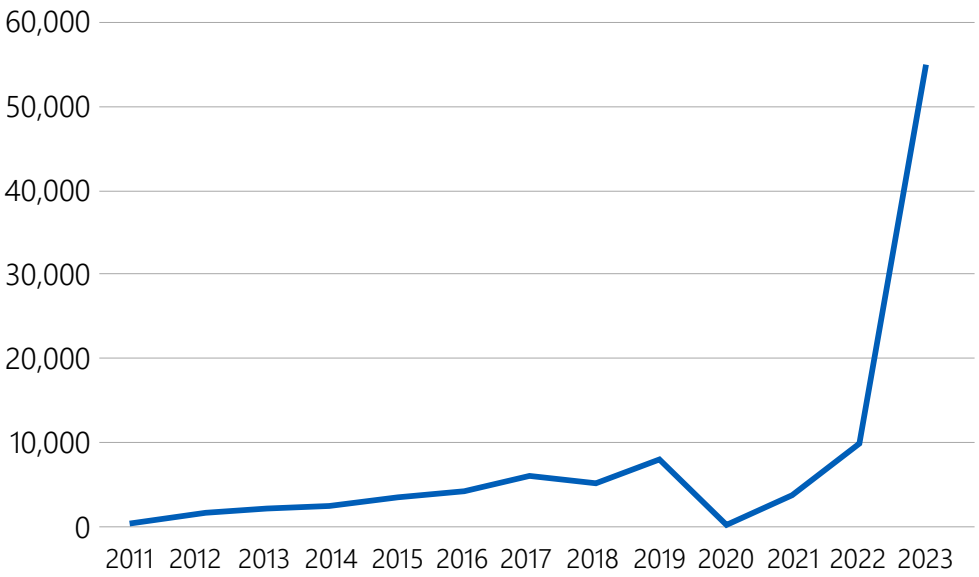
[109] Positive Hack Days attendance numbers compiled from open-source intelligence. Sourcing information available from CNA upon request.

[110] Positive Hack Days attendance numbers compiled from open-source intelligence.

[111] Andrei Soldatov and Irina Borogan, "Russia's Cybersecurity Companies Shrug Off Sanctions," Center for European Policy Analysis, Mar. 16, 2023, https://cepa.org/article/russias-cybersecurity-companies-shrug-off-sanctions/.

[112] "Positive Technologies Financials."

Figure 7. Positive Hack Days conference participants (in person, 2011–2023)



Source: Positive Hack Days attendance numbers, compiled from open-source intelligence. Sourcing information available from CNA upon request.

PT NGFW, a new Positive Technologies software and hardware appliance designed to protect corporate data networks of any size, as a key growth vector in 2025.[113] Positive Technologies supposedly acquired fewer than 500 customers in 2024, but for 2025, its sales target is to acquire 1,600 new customers—mostly derived from small, medium, and large businesses in the region.[114] It is possible that sanctions have hurt its business, but Positive Technologies' recent successes underscore that its affiliation with Russian security agencies has not impeded its growth in the region or elsewhere.

Case study analysis

Across all three case studies, we emphasize that Russian cybersecurity companies continue to willingly disclose their involvement with Russian government and security agencies. In fact, the companies in some cases describe their work for the state in their own marketing materials—for example, Security Code continues to tout its receipt of FSB licenses. This suggests that the Russian companies perceive branding or sales benefits from such disclosures. The Russian government's focus on securitization and on waging the war on Ukraine—and that it has oriented national spending in that direction—makes it probable that companies want to present themselves as pro-government to secure more government contracts. These same trends

[113] Positive Technologies, "Positive Technologies Unveils PT NGFW to Protect Businesses from Cyberattacks," Ptsecurity.com, Nov. 19, 2024, https://global.ptsecurity.com/about/news/pt-unveils-pt-ngfw-to-protect-businesses-from-cyberattacks; Positive Technologies, "PT NGFW," Ptsecurity.com, accessed Apr. 27, 2025, https://global.ptsecurity.com/products/ngfw; "Positive Technologies Financials."

[114] "Positive Technologies Financials."

make it probable that companies want to be vocal about their support for the government so that they receive financial benefits such as tax exemptions for IT workers operating in service of the state and, conversely, avoid the scrutiny that would come with running a major cyber business and failing to apply it to the Kremlin's wartime ends. It is also possible that some of the companies' executives and employees genuinely buy into the Kremlin's propaganda and want to be seen as supporting organizations like the FSB, GRU, and MVD.

The companies' revenue figures in 2022, 2023, and 2024 also indicate that the Russian cyber firms discussing working for the FSB, MOD, and other Russian state entities has not meaningfully undermined their business overseas—or that if the disclosures do undermine overseas business, the losses are still outweighed by the overall gains. On the one hand, this may align with overall trends in global perspectives on Russia's war against Ukraine. Some countries have been highly supportive of Russia's illegal invasion and war on Ukraine (e.g., Venezuela).[115] Others have taken mixed positions that have, at times, reflected the public's support for Russia or its lack of interest in prioritizing support for Ukraine (e.g., South Africa, Brazil, India).[116] Given these varied worldwide perspectives, customers in some countries may not care at all that a Russian private sector cyber firm contracts with the FSB, GRU, MOD, or another Russian military or intelligence agency. They may view these companies' work with the Russian government as a relatively better option than an American or European firm that may work with its respective government, or they may even view it positively, aligned with a positive perception of the Putin regime and the Russian government in general.

Nonetheless, companies or government agencies in other countries (e.g., Venezuela, Brazil, India) may not robustly support Ukraine yet still remain skeptical of Russian government contractors. We might also expect that cybersecurity customers in the countries in which Kaspersky, Security Code, and Positive Technologies are expanding may accept hiring a Russian cyber firm but not one (e.g., Kaspersky, Positive Technologies) that has been accused of supporting offensive cyber behavior that would hurt their networks and their bottom lines. However, the fact that these companies are openly advertising their work for Russian state agencies while expanding in Latin America, the Middle East, and elsewhere undermines these hypotheses for how well Russian cyber contractors can continue operating in key and dispersed markets.

In addition, we emphasize that these companies disclose their engagements with the Russian government, including in marketing materials, but have not provided much more information about the details of those engagements since 2022. Kaspersky has not suddenly posted blogs about its support for the FSB's offensive operations, Security Code remains vague on its website about how much of its work for agencies like the MOD is indeed defensive, and Positive Technologies, for its part, has not publicly discussed its reverse engineering capabilities, even though a media report from four years ago accused it of providing those capabilities

[115] See, for example, "Russia Signs Security, Energy Deals with Venezuela," *The Moscow Times*, Nov. 8, 2024, https://www.themoscowtimes.com/2024/11/08/russia-signs-security-energy-deals-with-venezuela-a86944.

[116] See, for example, Tim Mak, "South Africa's Belated Reckoning over the War in Ukraine," *Politico*, June 6, 2024, https://www.politico.com/news/magazine/2024/06/06/south-africa-ukraine-war-reckoning-00161508; Felipe Krause, "Explaining Brazil's Stance on the Ukraine War," *Bulletin of Latin American Research* 43, no. 4 (Sept. 2024), pp. 326–29, https://onlinelibrary.wiley.com/doi/10.1111/blar.13575; Ashley J. Tellis, "'What Is in Our Interest': India and the Ukraine War," Carnegie Endowment for International Peace, Apr. 25, 2022, https://carnegieendowment.org/research/2022/04/what-is-in-our-interest-india-and-the-ukraine-war?lang=en.

to the FSB. One likely—albeit partial—explanation for this observation is that the Russian government continues to classify the exact nature of its contracting with private sector Russian cyber firms. After all, what Kaspersky might be providing to the FSB could, in that scenario, reveal Russian cyber intelligence tradecraft or the targets in which the FSB is interested; similarly, documentation of which systems Security Code might be providing to which subunits of the MOD might expose information such as system architectures, operating systems in use, and gaps in defensive protections that the MOD would ostensibly want to keep secret.

There may also be a marketing reason the companies are not providing comprehensive information on their state support: to maintain some veneer of deniability, even if that deniability is implausible.

There may also be a marketing reason the companies are not providing comprehensive information on their state support: to maintain some veneer of deniability, even if that deniability is implausible. An acknowledgement from Kaspersky that it supports government clients, for instance (which it does now), is still different than Kaspersky announcing it might work with Russian intelligence agencies to carry out espionage (which it still denies). Even if the company could disclose that work, doing so might irk its Russian government clients (e.g., indicate a lack of discretion on the company's part or a desire to turn everything into marketing), give foreign governments more justification to sanction and ban it (e.g., increase momentum in Europe to expel Kaspersky products and services), and make some customers in countries like Brazil, India, and South Africa bristle at the outright admission of espionage support. It is plausible that customers intrigued by Kaspersky's global reach, talent base, pricing, services, and differentiation from other providers (e.g., US, European, Chinese, Israeli) may be fine with buying its services when there are strong hints and accusations of Russian government association but may be unable to internally justify making an acquisition when the risks to the customer's own networks—for example, that the FSB could backdoor all their systems—would be so great.

The complexity of this situation for Russian cyber companies indicates that their decisions to disclose their support for the state are not straightforward. They must navigate many competing considerations, from how their actions would be perceived domestically (including by their current and prospective state clients) to how their explicit disclosures of support might backfire in markets in which they are currently finding a greater foothold. Even Russian private sector cyber firms that do significant volumes of business with the government—and that are subject to ever more pressure from the state and the current Russian political environment—may still wish to claim, even dubiously, some amount of independence from the Putin regime.

From Russia's perspective, the Kremlin may be able to capitalize on companies' desires to present themselves as supporting the state (regardless of their motives for doing so). Cyber firms that already have contracts with Russian state entities may have an even greater appetite to increase the size and scope of those contracts—and to sign on additional Russian government organizations. Russian private sector cyber firms without government contracts may similarly now wish to expand into Russian government contracting, perceiving the potential financial, reputational, and other upsides of doing so.

Increased contracting with these firms could mean the Russian government is able to more actively leverage talent, capabilities, and technologies to further its offensive operations against the United States and the West, enhance defenses against Ukrainian and other cyber operations, and bolster its domestic cyber talent pool. Even if it does not expand its contracting with private sector cyber firms, the mere fact that many prominent Russian cyber firms are continuing to promote their government work—and, in some cases, repeat nationalistic rhetoric—strengthens the state's securitization of cyber issues. This proliferates state propaganda further and makes it more likely that nationalistic, technically talented youth will see cybersecurity as a viable, country-supporting career path, just as the Kremlin seems to desire.

As with all outsourcing of talent, capabilities, technologies, and even operations, greater Russian government contracting with cyber firms would also come with risks. The companies' desires to talk about their state work could hurt the Russian state's efforts to conceal the cyber proxies behind its espionage, disruptive cyber operations, and more; although the state could certainly classify contracts and pressure firms to remain quiet if it wanted, not every Russian government agency may conceal its connections with private actors as carefully as they currently are. Companies also want to make a profit, and government contracting for some Russian cyber firms (especially those hurt by sanctions and related business losses) may more or less be a means to an end. This could undermine the state's procuring of the best, most effective products and services to meet its needs. Lastly, in the long run, greater securitization and nationalization may hurt Russia's tech sector and impede the cyber sector's growth: if a national security use case is the only or even the most viable path to a Russian product's commercialization, many other Russian cyber innovations may fail to come to market around the world. Russian firms will lose out, and non-Russian competitors will fill the voids.

Looking Ahead

The private sector cyber firms in Russia's cyber ecosystem operate in an environment where the Kremlin can coerce companies to do its bidding—by using brute force (e.g., violence, intimidation, imprisonment), imposing legal restrictions, or simply pushing companies into low-paying contracts—and where many cyber firms work for the state outright. Their support, be it offensive, defensive, or merely educational, can therefore help support the Putin regime and its power projection efforts globally. How these companies operate matters greatly for the United States and the West.

The practices of Kaspersky, Security Code, and Positive Technologies underscore these dynamics. The first has been called a security threat by multiple Western countries and has been subject to multiple press reports about its support for Russian government intelligence collection. The second provides a variety of defensive services to civil and security agencies in Russia, as well as entities key to the Russian economy. The third has been publicly identified as a Russian intelligence contractor. The nature of these companies' relationships with the government appear to vary in substance (e.g., offensive versus defensive), in customer (e.g., the GRU versus the Ministry of Health), and in ability to maintain global reach simultaneously (e.g., globally versus mostly focused on Russia). Despite their associations with the Russian state, all three companies ended 2024 with their highest revenues to date.

However, these three companies' revenue figures do not come close to the financial figures of the largest American cybersecurity firms; CrowdStrike, for example, made $3.1 billion in 2024, and Recorded Future was bought in 2024 by Mastercard for $2.65 billion.[117] If Russian cyber firms are successful in large markets, such as Brazil and India, in the coming years, they could become more competitive. Simultaneously, it remains to be seen whether their growing footholds in key markets and their continued revenue streams from the Russian state will allow them to grow to the size of some of their largest Western competitors, which suggests that competitive edges and shortfalls coexist for Russian private sector cyber firms.

To better evaluate the role of Russian private sector cyber firms in Russia's cyber web, analysts, practitioners, and policy-makers should consider further analysis of the following questions:

1. **How can companies better identify Russian providers in supply chains and determine whether they present risks?** Evaluating which Russian firms sit below an acceptable risk threshold for engagement is difficult, considering that many are susceptible to state influence or conceal their support for state operations. Furthermore, many companies' technology supply chains are complex, which can make it exceedingly challenging to understand which vendor, in which part of the supply chain, could potentially be using technology from a state-support-

[117] "CrowdStrike Reports Fourth Quarter and Fiscal Year 2024 Financial Results," Crowdstrike.com, Mar. 5, 2024, https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-fourth-quarter-and-fiscal-year-2024; "Mastercard Invests in Continued Defense of Global Digital Economy with Acquisition of Recorded Future," Mastercard.com, Sept. 12, 2024, https://www.mastercard.com/news/press/2024/september/mastercard-invests-in-continued-defense-of-global-digital-economy-with-acquisition-of-recorded-future/.

ing Russian cyber company. Building out more detailed supply chain risk frameworks and mitigation paths could help critical infrastructure, emerging technology, and defense firms better protect themselves from vectors of compromise.

2. **In which regions and markets are Russian cyber firms expanding the most, and what can their sales pitches and successes teach the United States and the West?** Many Russian cyber companies do not break their public financials down by region. Better understanding Russian cyber firms' performance in different regions, such as Latin America and the Middle East, and in key markets, such as Singapore, Brazil, India, and South Africa, could help the United States and the West better evaluate how Russian cyber firms are growing and adapting to wartime conditions. Analyzing Russian firms that contract with the state could reveal which parts of the world are opening themselves up to the Russian supply chain or cyber compromise through private sector technology. Studying which sales pitches from Russian firms are landing where and why could be valuable for the US government's defensive and diplomatic planning.
3. **What would a more analytically robust, comprehensive assessment of possible Russian private company support for the Kremlin look like?** For example, as scholars such as Jason Healey have pointed out, treating nonstate actors as either government involved or not government involved does not adequately capture the range of potential relationships at play and how they can evolve.[118] In Russia's case, the three examples explored in this paper show that bucketing state contractors into "offensive" or "defensive" is reductive; some firms may do both, and some may do neither. Future research and analysis should explore how educational and recruitment efforts fit into the spectrum. Fleshing out these concepts could enable more tailored analysis of the Russian state cyber contractors of greatest concern to the United States and the West.

The Russian cyber threat to the United States and the West is not going away. Cultivating a sharper, more informed, and more nuanced understanding of the various actors, structures, incentives, activities, and relationships in Russia's cyber web—including private sector cyber firms that work with the state—will allow a better response to these risks in the future.

[118] Healey, *Beyond Attribution*.

Figures

Abbreviations

BIS	Bureau of Industry and Security
CCI	critical information infrastructure (entities)
DHS	US Department of Homeland Security
FSB	Federal Security Service
FSO	Federal Protective Service
GRU	military intelligence agency
JSC	Joint Stock Company
MEPhI	National Research Nuclear University
MOD	Ministry of Defense
MPEI	National Research University
MVD	Ministry of Internal Affairs
NGFW	Next-Generation Firewall
PJSC VTB	Public Joint Stock Company VTB
SVR	Foreign Intelligence Service
UK	United Kingdom
VEB	Vnesheconombank

References

"'Aerokitties' Fly in Swarms. How Higher Education Programs in Drone Technology Service Military Objectives." T-invariant.org. Feb. 20, 2025. https://t-invariant.org/2025/02/aerokitties-fly-in-swarms-how-higher-education-programs-in-drone-technology-serve-military-objectives/.

Amante, Angelo. "Italy Set to Curb Use of Russian Anti-Virus Software in Public Sector." Reuters. Mar. 17, 2022. https://www.reuters.com/technology/italy-set-curb-use-russian-anti-virus-software-public-sector-2022-03-17/.

Artificial Intelligence in Russia: Issue 8, August 14, 2020. CNA. Aug. 2020. https://apps.dtic.mil/sti/trecms/pdf/AD1120632.pdf.

Bajak, Frank, and Matt O'Brien. "Sanctioned Russian IT Firm Was Partner with Microsoft, IBM." Associated Press. Apr. 15, 2021. https://apnews.com/article/business-europe-hacking-russia-dd8c331ff30d366ea4f5d828e788c307.

Baker, Kurt. "What Is Ransomware as a Service (RaaS)?" Crowdstrike.com. Jan. 30, 2023. https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

Balforth, Tom. "Exclusive: Russian Hackers Were Inside Ukraine Telecoms Giant for Months." Reuters. Jan. 5, 2024. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

Belovodyev, Daniil, Anton Bayev, and Systema. "Inside the Obscure Russian Agency That Censors the Internet: An RFE/RL Investigation." Radio Free Europe/Radio Liberty. Feb. 9, 2023. https://www.rferl.org/a/russia-agency-internet-censorship/32262102.html.

Bergman, Ronan, and Kate Conger. "Chinese Hackers Tried to Steal Russian Defense Data, Report Says." *New York Times*. May 19, 2022. https://www.nytimes.com/2022/05/19/world/asia/china-hackers-russia.html.

Bowen, Andrew S. *Russian Law Enforcement and Internal Security Agencies*. IF11647 Congressional Research Service. Sept. 2020. https://www.congress.gov/crs-product/IF11647.

Brewster, Thomas. "Watch as Hackers Hijack WhatsApp Accounts via Critical Telecom Flaws." *Forbes*. June 1, 2016. https://www.forbes.com/sites/thomasbrewster/2016/06/01/whatsapp-telegram-ss7-hacks/?sh=3e2c9546178b.

Chislova, Olga, and Marina Sokolova. "Cybersecurity in Russia." *International Cybersecurity Law Review* 2 (2021): 245–51. https://link.springer.com/article/10.1365/s43439-021-00032-9.

"CII Protection." Satel.ru. Accessed Apr. 27, 2025. https://satel.ru/en/integration/cii-protection/.

Contemporary Biographies in Communications & Media. Englewood Cliffs: Salem Press, 2014. https://web.archive.org/web/20150426074648/http://salempress.com/store/pdfs/bios_com_pgs.pdf.

"CrowdStrike Reports Fourth Quarter and Fiscal Year 2024 Financial Results." Crowdstrike.com. Mar. 5, 2024. https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-fourth-quarter-and-fiscal-year-2024.

Decree of the President of Ukraine No. 549. Sept. 16, 2025. https://www.president.gov.ua/documents/5492015-19437.

"Dimitrovgrad Engineering and Technical Institute—Branch of Federal Autonomous Higher Vocational Educational Institution 'National Research Nuclear University MEPhI.'" Cluster-dgrad.ru. Archived Apr. 9, 2025. https://web.archive.org/web/20250409170129/https://cluster-dgrad.ru/en/members-project/35-national-research-nuclear-university-mifi.

Efron, Sonni. "Murder for Hire in Moscow: A Wave of Contract Killings Has Russians on Edge. Businessmen Are the Prime Targets of Brazen Hit Men, Who Style Themselves After American Gangsters." *Los Angeles Times*. Aug. 13, 1993. https://www.latimes.com/archives/la-xpm-1993-08-13-mn-23397-story.html.

Esposito, Jeffrey. "A Transparent Move in North America." Usa.kaspersky.com. Dec. 13, 2021. https://usa.kaspersky.com/blog/kaspersky-transparency-center-north-america/25939/.

Europol. "No More Ransom Update: Belgian Federal Police Releases Free Decryption Keys for the Cryakl Ransomware." Europol.europa.eu. Feb. 9, 2018. https://www.europol.europa.eu/media-press/newsroom/news/no-more-ransom-update-belgian-federal-police-releases-free-decryption-keys-for-cryakl-ransomware.

Federal State Budgetary Institution "4th Central Research Institute" of the Ministry of Defense of the Russian Federation [« ФГБУ "4 Центральный научно-исследовательский институт" Министерства обороны Российской Федерации »]. Mpei.ru. Jan. 4, 2019. https://web.archive.org/web/20250409171233/https://mpei.ru/Structure/uchchast/educadmin/deptf/Lists/jobList/NewDispForm.aspx?ID=460&RootFolder=%2FStructure%2Fuchchast%2Feducadmin%2Fdeptf%2FLists%2FjobList&Source=https%3A%2F%2Fmpei%2Eru%2FStructure%2Fuchchast%2Feducadmin%2Fdeptf%2FPages%2Fjob%2Easpx%3Fp%3D5.

Franceschi-Bicchierai, Lorenzo. "Kaspersky Says It's Closing Down Its UK Office and Laying Off Dozens." *TechCrunch*. Oct. 8, 2024. https://techcrunch.com/2024/10/08/kasperksy-says-its-closing-down-its-uk-office-and-laying-off-dozens/.

Galeotti, Mark. *The Law Enforcement Agencies: Russian Domestic Security and International Implications*. George C. Marshall European Center for Security Studies. Feb. 2020. https://www.marshallcenter.org/en/publications/security-insights/law-enforcement-agencies-russian-domestic-security-and-international-implications-0.

"Germany Warns Against Russian Anti-Virus Use." BBC. Mar. 15, 2022. https://www.bbc.com/news/technology-60738208.

Global Entrepreneurship and the Successful Growth Strategies of Early-Stage Companies. World Economic Forum. 2011. https://www.iese.edu/media/research/pdfs/ESTUDIO-137.pdf.

"Government Takes Russia's NTV." ABC News. Apr. 14, 2001. https://abcnews.go.com/International/story?id=81235&page=1.

"The GRU's Disruptive Playbook." Mandiant. July 12, 2023. https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook.

Hakala, Janne, and Jazlyn Melnychuk. *Russia's Strategy in Cyberspace*. NATO Strategic Communications Centre of Excellence. June 2021. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.

Harris, Shane, and Gordon Lubold. "Russia Has Turned Kaspersky Software into Tool for Spying." *Wall Street Journal*. Oct. 11, 2017. https://www.wsj.com/articles/russian-hackers-scanned-networks-world-wide-for-secret-u-s-data-1507743874.

Healey, Jason. *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*. Atlantic Council. Feb. 2012. https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

"How Russia's GRU Set Up a Fake Private Military Company for Its War in Ukraine." Radio Free Europe/Radio Liberty. Oct. 10, 2023. https://www.rferl.org/a/russia-gru-fake-private-military-company-ukraine-redut-investigation/32630705.html.

Irwin, Kate. "Kaspersky Shuts Down US Operations Following Nationwide Ban." *PC Mag*. July 16, 2024. https://www.pcmag.com/news/kaspersky-shutting-down-us-operations-following-nationwide-ban.

Johnson, Derek B. "Judge Upholds Government Ban on Kaspersky Products." Nextgov/FCW. May 30, 2018. https://www.nextgov.com/cybersecurity/2018/05/judge-upholds-government-ban-on-kaspersky-products/196295/.

Kadlecová, Lucie. "Russian-Speaking Cyber Crime: Reasons Behind Its Success." *European Review of Organised Crime* 2, no. 2 (2015): 104–21. https://standinggroups.ecpr.eu/sgoc/wp-content/uploads/sites/51/2020/01/kadlecova.pdf.

Kaspersky. "An Analysis of Hacker Mentality." Encyclopedia.kaspersky.com. 2004. https://web.archive.org/web/20241210093016/https://encyclopedia.kaspersky.com/knowledge/an-analysis-of-hacker-mentality/.

Kaspersky. "Brief Company History." Kaspersky.com. Accessed Jan. 24, 2025. https://web.archive.org/web/20250124102647/https://esg.kaspersky.com/en/about-company/brief-history.

Kaspersky. "Company Overview." Kaspersky.com. Accessed Mar. 28, 2025. https://web.archive.org/web/20250328105919/https://www.kaspersky.com/about/company.

Kaspersky. "Contáctanos." Latam.kaspersky.com. Accessed Apr. 7, 2025. https://web.archive.org/web/20250407161533/https://latam.kaspersky.com/about/contact.

Kaspersky. "Kaspersky Lab Announces 4% Revenue Growth to $726 Million in 2018." Kaspersky.com. Feb. 19, 2019. https://www.kaspersky.com/about/press-releases/kaspersky-lab-announces-4-percent-revenue-growth-to-726-million-dollars-in-2018.

Kaspersky. "Kaspersky Relocates Cyberthreat-Related Data Processing for Users in Latin America and Middle East to Switzerland and Re-Certifies Its Data Services by TÜV AUSTRIA." Kaspersky.com. Apr. 14, 2022. https://www.kaspersky.com/about/press-releases/kaspersky-relocates-cyberthreat-related-data-processing-for-users-in-latin-america-and-middle-east-to-switzerland-and-re-certifies-its-data-services-by-tuv-austria.

Kaspersky. "Kaspersky Reports Financial Results with Stable Business Growth in 2020." Kaspersky.com. Apr. 19, 2021. https://www.kaspersky.com/about/press-releases/kaspersky-reports-financial-results-with-stable-business-growth-in-2020.

Kaspersky. "Kaspersky Reports 2019 Financial Results." Kaspersky.com. July 24, 2020. https://www.kaspersky.com/about/press-releases/kaspersky-reports-2019-financial-results.

Kaspersky. "Kaspersky Reports 2021 Financial Results." Kaspersky.com. June 10, 2022. https://www.kaspersky.com/about/press-releases/kaspersky-reports-2021-financial-results.

Kaspersky. "Kaspersky Reports 2023 Financial Results with 11% Business Growth." Kaspersky.com. June 20, 2024. https://www.kaspersky.com/about/press-releases/kaspersky-reports-2023-financial-results-with-11-business-growth.

Kaspersky. "Kaspersky Reports 2024 Financial Results with Record Revenue." Kaspersky.com. Apr. 9, 2025. https://www.kaspersky.com/about/press-releases/kaspersky-reports-2024-financial-results-with-record-revenue.

Kaspersky. "Kaspersky Statement on Compliance in the US Following ICTS Final Determination." Usa.kaspersky.com. July 18, 2024. https://usa.kaspersky.com/about/press-releases/kaspersky-statement-on-compliance-in-the-us-following-icts-final-determination.

Kaspersky. "Kaspersky Transparency Center." Kaspersky.com. Archived Apr. 21, 2025. https://www.kaspersky.com/transparency-center-offices.

Kaspersky. "No More Ransom: Law Enforcement and IT Companies Join Forces to Fight Ransomware." Kaspersky.com. July 25, 2016. https://web.archive.org/web/20241008112716/https://www.kaspersky.com/about/press-releases/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware.

Kaspersky. "Report*: In 2014 Kaspersky Lab Grew Faster Than the Market." Kaspersky.com. Jan. 8, 2016. https://www.kaspersky.com/about/press-releases/report-in-2014-kaspersky-lab-grew-faster-than-the-market.

Kaspersky Lab. "Company Profile." Kaspersky.com. 2014. https://web.archive.org/web/20250407173445/https://media.kaspersky.com/en/Corporate_Presentation_Q12014.pdf.

"Kaspersky Lab Closes Regional Office in Ukraine." TASS. Dec. 14, 2016. https://tass.com/economy/919394.

"Kaspersky Lab Reports Growth Despite U.S. Government Ban." Radio Free Europe/Radio Liberty. Jan. 20, 2018. https://www.rferl.org/a/kaspersky-reports-8-percent-revenue-growth-despite-us-government-ban-software-/28986290.html.

"Kaspersky Lab Transparency Center Opens in Colombia [В Колумбии открылся Центр прозрачности «Лаборатории Касперского»]." D-russia.ru. Nov. 18, 2024. https://d-russia.ru/v-kolumbii-otkrylsja-centr-prozrachnosti-laboratorii-kasperskogo.html.

Kaspersky, Eugene. "What Wired Is Not Telling You—A Response to Noah Shachtman's Article in Wired Magazine." Eugene.kaspersky.com. July 25, 2012. https://web.archive.org/web/20120726135749/https://eugene.kaspersky.com/2012/07/25/what-wired-is-not-telling-you-a-response-to-noah-shachtmans-article-in-wired-magazine/.

Kofman, Michael, Anya Fink, Dmitry Gorenburg, Mary Chesnut, Jeffrey Edmonds, and Julian Waller. *Russian Military Strategy: Core Tenets and Operational Concepts*. CNA. DRM-2021-U-029755-1Rev. Oct. 2021. https://www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts.

Krause, Felipe. "Explaining Brazil's Stance on the Ukraine War." *Bulletin of Latin American Research* 43, no. 4 (Sept. 2024): 326–29. https://onlinelibrary.wiley.com/doi/10.1111/blar.13575.

Krebs, Brian. "Notorious Malware, Spam Host 'Prospero' Moves to Kaspersky Lab." Krebsonsecurity.com. Feb. 28, 2025. https://krebsonsecurity.com/2025/02/notorious-malware-spam-host-prospero-moves-to-kaspersky-lab/.

Kuranda, Sarah. "Kaspersky Removed from GSA Schedule, Limiting Federal Sales for Its Security Software." Crn.com. July 12, 2017. https://www.crn.com/news/security/300088591/kaspersky-removed-from-gsa-schedule-limiting-federal-sales-for-its-security-software.

Lennon, Mike. "Kaspersky Lab 2011 Revenue Tops $612 Million, but No IPO in Sight." Securityweek.com. Feb. 10, 2012. https://www.securityweek.com/kaspersky-lab-2011-revenue-tops-612-million-no-ipo-sight/.

Levy, Clifford J. "In Hard Times, Russia Tries to Reclaim Industries." *New York Times*. Dec. 7, 2008. https://www.nytimes.com/2008/12/08/world/europe/08kremlin.html.

Lindsay, Jon R. "Proxy Wars: Control Problems in Irregular Warfare and Cyber Operations." *International Studies Association Annual Meeting*. Apr. 2013. http://files.isanet.org/ConferenceArchive/1a381131aa014f02ab15a7b55b8509d7.pdf.

"LLC Security Code." Opensanctions.org. Accessed Apr. 27, 2025. https://www.opensanctions.org/entities/NK-6sfEe2d9qSQzprVpJysUFH/.

Lubold, Gordon, and Shane Harris. "Russian Hackers Stole NSA Data on US Cyber Defense." *Wall Street Journal*. Oct. 5, 2017. https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

Macalister, Terry, and Tom Parfitt. "$20bn Gas Project Seized by Russia." *The Guardian*. Dec. 12, 2006. https://www.theguardian.com/world/2006/dec/12/business.oil.

Mak, Tim. "South Africa's Belated Reckoning over the War in Ukraine." *Politico*. June 6, 2024. https://www.politico.com/news/magazine/2024/06/06/south-africa-ukraine-war-reckoning-00161508.

"Mastercard Invests in Continued Defense of Global Digital Economy with Acquisition of Recorded Future." Mastercard.com. Sept. 12, 2024. https://www.mastercard.com/news/press/2024/september/mastercard-invests-in-continued-defense-of-global-digital-economy-with-acquisition-of-recorded-future/.

Matlack, Carol, Michael A. Riley, and Jordan Robertson. "The Company Securing Your Internet Has Close Ties to Russian Spies." Bloomberg. Mar. 19, 2015. https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Carnegie Endowment for International Peace. 2018.

Military Study Center [Военный учебный центр (ВУЦ)]. Sut.ru. Archived Apr. 9, 2025. https://web.archive.org/web/20250409173833/https://www.sut.ru/university/structure/vuc.

Military Study Center [Военный учебный центр (ВУЦ)]. Vuc.mpei.ru. Archived Apr. 9, 2025. https://web.archive.org/web/20250409171215/https://vuc.mpei.ru/Pages/default.aspx.

Military Study Center at St. Petersburg State Communications University [Военный Учебный Центр СПБГУТ]. Mil.spbsut.ru. Archived Apr. 9, 2025. https://web.archive.org/web/20250403120156/https://mil.spbsut.ru/.

"The Ministry of Defense Will Consider the Idea of Creating Military Training Centers at the Universities of the Ministry of Digital Development [« Минобороны рассмотрит идею создания военно-учебных центров в вузах Минцифры »]." TASS. Dec. 26, 2023. https://tass.ru/obschestvo/19629995.

"Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses." Department of Homeland Security. 82 *FR* 43782. Sept. 19, 2017. https://www.federalregister.gov/documents/2017/09/19/2017-19838/national-protection-and-programs-directorate-notification-of-issuance-of-binding-operational.

Omelicheva, Mariya Y. *Repression Trap: The Mechanism of Escalating State Violence in Russia*. Center for Strategic & International Studies. July 2021. https://www.csis.org/analysis/repression-trap-mechanism-escalating-state-violence-russia.

On the Security of the Critical Information Infrastructure of the Russian Federation. Russian Federal Law No. 187-FZ. July 26, 2017. https://www.prlib.ru/en/node/692141.

O'Neill, Patrick Howell. "Kaspersky's North American Operations Undergoes Shuffle; Head of PR Leaves Company." CyberScoop. Oct. 11, 2017. https://cyberscoop.com/kaspersky-north-america-jennifer-wood/.

O'Neill, Patrick Howell. "The $1 Billion Russian Cyber Company That the US Says Hacks for Moscow." *MIT Technology Review*. Apr. 15, 2021. https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/.

Perlroth, Nicole, and Scott Shane. "How Israel Caught Russian Hackers Scouring the World for US Secrets." *New York Times*. Oct. 10, 2017. https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

Positive Technologies. "About Us." Ptsecurity.com. Archived Apr. 8, 2025. https://web.archive.org/web/20250408173347/https://global.ptsecurity.com/about.

Positive Technologies. "Contacts." Ptsecurity.com. Archived Apr. 21, 2025. https://web.archive.org/web/20250421163932/https://global.ptsecurity.com/about/contacts.

Positive Technologies. "Positive Technologies Unveils PT NGFW to Protect Businesses from Cyberattacks." Ptsecurity.com. Nov. 19, 2024. https://global.ptsecurity.com/about/news/pt-unveils-pt-ngfw-to-protect-businesses-from-cyberattacks.

Positive Technologies. "PT NGFW." Ptsecurity.com. Accessed Apr. 27, 2025. https://global.ptsecurity.com/products/ngfw.

Positive Technologies. "Our Clients [«Наши клиенты»]." Ptsecurity.com. Archived Apr. 3, 2025. https://web.archive.org/web/20250403060911/https://www.ptsecurity.com/ru-ru/about/clients/#gos-uchrezhdeniya.

"Positive Technologies Financials." Tadviser.com. Accessed May 2025. https://tadviser.com/index.php/Article:Positive_Technologies_financials.

Pulsen, Kevin. "This Hacker Party Is Ground Zero for Russia's Cyberspies." *Daily Beast*. Aug. 3, 2018. https://www.thedailybeast.com/this-hacker-party-is-ground-zero-for-russias-cyberspies-3/.

Riehle, Kevin P. "Ignorance, Indifference, or Incompetence: Why Are Russian Covert Actions So Easily Unmasked?" *Intelligence and National Security* 39, no. 5 (Jan. 2024): 864–78. https://www.tandfonline.com/doi/full/10.1080/02684527.2023.2300165.

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

Rodeheffer, Luke. "Russia Ramps Up Cybersecurity Systems." *Eurasia Daily Monitor* 22, no. 15 (Feb. 6, 2025). https://jamestown.org/program/russia-ramps-up-cybersecurity-systems/.

"Rosenergoatom Concern JSC: Overview." Globaldata.com. Accessed Apr. 21, 2025. https://www.globaldata.com/company-profile/rosenergoatom-concern-jsc/.

"Russia Signs Security, Energy Deals with Venezuela." *The Moscow Times*. Nov. 8, 2024. https://www.themoscowtimes.com/2024/11/08/russia-signs-security-energy-deals-with-venezuela-a86944.

Schachtman, Noah. "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals." *WIRED*. July 23, 2012. https://www.wired.com/2012/07/ff-kaspersky/.

Schmitt, Michael N., and Liis Vihul. "Proxy Wars in Cyberspace: The Evolving International Law of Attribution." *Fletcher Security Review* 1, no. 53 (2014): 54–73. https://ccdcoe.org/library/publications/proxy-wars-in-cyberspace-the-evolving-international-law-of-attribution/.

Security Code. "About the Company [« О компании »]." Securitycode.ru. Archived June 19, 2021. https://web.archive.org/web/20210619151914/https://www.securitycode.ru/company/.

Security Code. "About Us." Securitycode.net. Archived Apr. 9, 2025. https://web.archive.org/web/20250409155741/https://www.securitycode.net/company/.

Security Code. "Clients [« Клиенты »]." Securitycode.ru. Archived Aug. 4, 2021. https://web.archive.org/web/20210804223837/https://www.securitycode.ru/clients/.

Security Code. "Education [« Обучение »]." Securitycode.ru. Archived Sept. 16, 2021. https://web.archive.org/web/20210916230243/https://www.securitycode.ru/company/training/.

Security Code. "Licenses [« Лицензии »]." Securitycode.ru. Archived Aug. 4, 2021. https://web.archive.org/web/20210804210812/https://www.securitycode.ru/company/company-s-licenses/.

Sherman, Justin. "Russia's Internet Censor Is Also a Surveillance Machine." Council on Foreign Relations. Sept. 28, 2022. https://www.cfr.org/blog/russias-internet-censor-also-surveillance-machine.

Sherman, Justin. "Russia's Largest Hacking Conference: Biggest Hits from Positive Hack Days 2023." Margin Research. Dec. 5, 2023. https://margin.re/2023/12/russias-largest-hacking-conference-biggest-hits-from-positive-hack-days-2023-2/.

Sherman, Justin. "Russia's Largest Hacking Conference Reflects Isolated Cyber Ecosystem." Brookings Institution. Jan. 12, 2023. https://www.brookings.edu/articles/russias-largest-hacking-conference-reflects-isolated-cyber-ecosystem/.

Sherman, Justin. *Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior*. Atlantic Council. Sept. 2022. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/.

"Solar Security and Positive Technologies to Create Cybersecurity Centers [« Solar Security и Positive Technologies займутся созданием центров кибербезопасности »]." Astera.ru. Nov. 20, 2017. https://astera.ru/news/solar-security-i-positive-technologies-zajmutsya-sozdaniem-tsentrov-k/.

Soldatov, Andrei, and Irina Borogan. *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*. Center for European Policy Analysis. Sept. 2022. https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

Soldatov, Andrei, and Irina Borogan. "Russia's Cybersecurity Companies Shrug Off Sanctions." Center for European Policy Analysis. Mar. 16, 2023. https://cepa.org/article/russias-cybersecurity-companies-shrug-off-sanctions/.

Stronski, Paul. "Implausible Deniability: Russia's Private Military Companies." Carnegie Endowment for International Peace. June 2, 2020. https://carnegieendowment.org/posts/2020/06/implausible-deniability-russias-private-military-companies?lang=en.

Takahashi, Dean. "Private Equity Firm General Atlantic Takes $200M Stake in Security Software Vendor Kaspersky Lab." Venture Beat. Jan. 19, 2011. https://venturebeat.com/security/private-equity-firm-general-atlantic-takes-200m-stake-in-security-software-vendor-kaspersky-lab/.

Tellis, Ashley J. "'What Is in Our Interest': India and the Ukraine War." Carnegie Endowment for International Peace. Apr. 25, 2022. https://carnegieendowment.org/research/2022/04/what-is-in-our-interest-india-and-the-ukraine-war?lang=en.

Timberg, Craig, Ellen Nakashima, Hannes Munzinger, and Hakan Tanriverdi. "Secret Trove Offers Rare Look into Russian Cyberwar Ambitions." *Washington Post*. Mar. 30, 2023. https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/.

"Ukraine Bans Russian Anti-Virus Kaspersky Lab Software—Cabinet of Ministers." TASS. Sept. 25, 2015. https://tass.com/economy/823636.

US Bureau of Industry & Security. "Commerce Department Prohibits Russian Kaspersky Software for US Customers." BIS.gov. June 20, 2024. https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-u.s.-customers.

US Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Justice.gov. Oct. 19, 2020. https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

US Department of the Treasury. "On Second Anniversary of Russia's Further Invasion of Ukraine and Following the Death of Aleksey Navalny, Treasury Sanctions Hundreds of Targets in Russia and Globally." Treasury.gov. Feb. 23, 2024. https://home.treasury.gov/news/press-releases/jy2117.

US Department of the Treasury. "Treasury Sanctions Entities in Iran and Russia That Attempted to Interfere in the US 2024 Election." Treasury.gov. Dec. 31, 2024. https://home.treasury.gov/news/press-releases/jy2766.

US Department of the Treasury. "Treasury Sanctions Kaspersky Lab Leadership in Response to Continued Cybersecurity Risks." Treasury.gov. June 21, 2024. https://home.treasury.gov/news/press-releases/jy2420.

US Department of the Treasury. "Treasury Sanctions Russia with Sweeping New Sanctions Authority." Treasury.gov. Apr. 15, 2021. https://home.treasury.gov/news/press-releases/jy0127.

US Federal Communications Commission. "FCC Expands List of Equipment and Services That Pose Security Threat." FCC.gov. Mar. 25, 2022. https://www.fcc.gov/document/fcc-expands-list-equipment-and-services-pose-security-threat.

Vicens, AJ. "Can Kaspersky Survive the Ukraine War?" CyberScoop. Sept. 28, 2022. https://cyberscoop.com/kaspersky-ban-europe-russia-government/.

Volkov, Vadim. *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism*. Ithaca: Cornell University Press, 2016.

White House. *National Cybersecurity Strategy*. Mar. 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

White House. *National Cyber Strategy of the United States of America*. Sept. 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Wilde, Gavin, and Justin Sherman. *No Water's Edge: Russia's Information War and Regime Security*. Carnegie Endowment for International Peace. Jan. 2023. https://carnegieendowment.org/research/2023/01/no-waters-edge-russias-information-war-and-regime-security?lang=en.

Zetter, Kim. "Sanctioned Firm Accused of Helping Russian Intelligence Was Part of Microsoft's Early Vuln Access Program—MAPP." Zero Day. Apr. 16, 2021. https://www.zetter-zeroday.com/sanctioned-firm-accused-of-helping/.

PAGE INTENTIONALLY BLANK

This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

About the author

Justin Sherman is the founder and CEO of Global Cyber Strategies, a Washington, DC–based research and advisory firm. He is also a nonresident senior fellow at the Atlantic Council's Cyber Statecraft Initiative and sanctioned by the Russian government.

Dedicated to the Safety and Security of the Nation

www.cna.org

About CNA

CNA is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the Department of the Navy's federally funded research and development center (FFRDC)—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform the decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and innovative methods to support federal, state, and local government officials as they work to advance national and homeland security.

DOP-2025-U-042210-Final