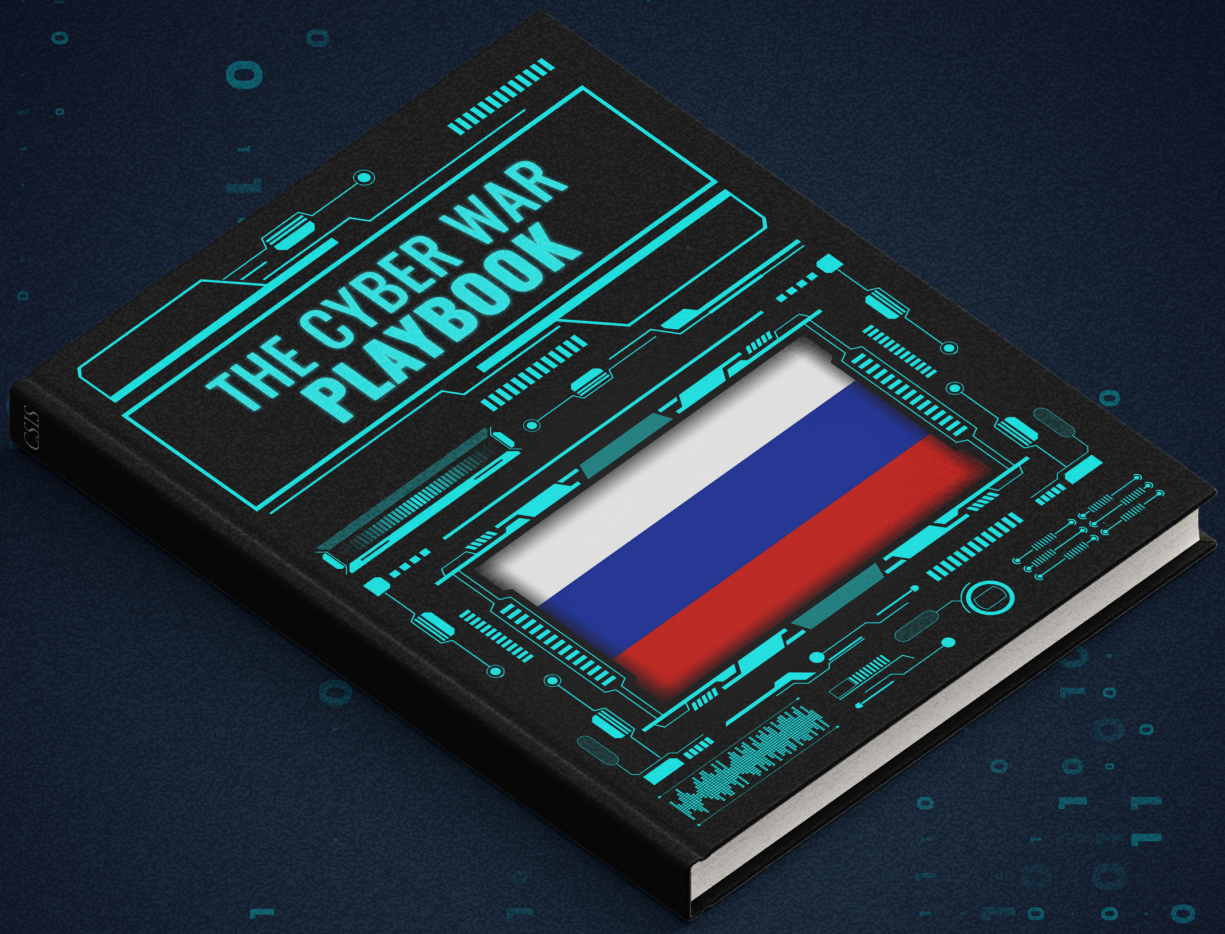
SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 2: Evaluating Russia's Cyber Strategy



Julia Dickson Emily Harding

A Report of the CSIS Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 2: Evaluating Russia's Cyber Strategy

AUTHORS
Julia Dickson
Emily Harding

A Report of the CSIS Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgements

The authors would like to extend their gratitude to those who agreed to be interviewed and to their foreign partners who contributed valuable insights from the front lines of this fight. The authors would also like to thank Nicole Aandahl for graciously providing valuable feedback, Susan Hines for helping with the project contract, and the CSIS iDeas Lab for offering their design expertise.

This report is made possible by project support from the Smith Richardson Foundation.

Contents

Authors' Note About the Series

Photo Source: Roman/Adobe Stock

This report is part of a series on the future of cyber warfare. This part of the series examines how Russia fights in the cyber domain, including the core elements of Moscow's strategy for conducting cyber operations, how that strategy fits in a larger foreign policy context, and who the frontline fighters are in this new mode of conflict.

Part 1 of this series offers a broad introduction to the report, covers key takeaways from the comparative studies and wargames, and summarizes the authors' recommendations. Parts 2, 3, and 4 examine how Russia, China, and Iran, respectively, fight in the cyber domain, and Part 5 examines U.S. cyber practices. Part 6 tests how U.S. policymakers view cyber operations as part of the spectrum of war, peace, and irregular warfare, illuminated by a set of wargames. Finally, Part 7 fully explains the new playbook that will close the gap between how the United States and its adversaries fight and succeed in the cyber domain.

Overview of Russia's Cyber Playbook

The principal goals driving Russia's cyber strategy across the spectrum of conflict are clear: disruption, destruction, and control of information. Russian actors perpetrated the earliest known cyberattacks, and Russia has continued to be a leader in cyber activity.

Moscow views cyber operations and information operations as indivisible. As a result, Russia's targets include government networks for the purposes of espionage, critical infrastructure for operational preparation of the environment (OPE), and communication mechanisms to manipulate the psyche of an adversary's population. To describe its activities in cyberspace, Moscow employs the term *informatsionnoe protivoborstvo* (IPb), which roughly translates to "information confrontation." IPb describes a much broader range of activities than Western conceptions of "cyberwar." As the NATO Strategic Communications Centre of Excellence describes it, "More than any other country, Russia attempts to achieve cognitive effects when conducting cyber operations."[1] While this project focuses more on cyber operations than on information operations, one central finding of the research is that U.S. adversaries—Russia in particular—view these operations as inseparable.[2]

The strengths and weaknesses of Russian cyber strategy have been made evident by its war in Ukraine. As Washington and London warned Kyiv and other European capitals that a full-scale Russian invasion of Ukraine looked likely, a hidden war was beginning in the cyber domain. Before the invasion began, Russia was retreading tools used in previous attacks on Ukraine to undermine the basic functioning of Ukrainian society. Russian-affiliated cyber actors went after oil and gas companies, banks, and the websites of the Ukrainian Ministry of Defence.[3] When the conflict

shifted from OPE to open war, Russia's efforts refocused on government targets, communication infrastructure, power, and media.[4]

But few disastrous effects materialized. The apparent lack of disruption was not from a lack of Russian effort. This time, Ukraine was ready, and its defenses proved potent. Ukraine had suffered from Russian aggression in the cyber domain for years and was aware of the need for resilience.[5] Therefore, Kyiv had created redundant internet infrastructure, trained talented cyber defenders, and recruited allies in Western governments and technology companies. Professionals at Microsoft, Mandiant, and other firms sat (virtually and literally) side by side with Ukrainian defenders, limiting damage and restoring critical systems.[6]

In many ways, Russia's war against Ukraine is a unique case that could provide false reassurance that a cyber conflict between Moscow and the United States would be inconsequential. That hope would be misplaced. The United States and its allies have not prioritized developing resilient systems to the same degree Ukraine has, and they do not have the years of practice defending against Russian attacks that Ukraine has. The *Microsoft Digital Defense Report 2023*, for instance, found that 48 percent of Russian state and state-affiliated cyberattacks were against Ukrainian institutions, a phenomenon that Ukraine has been grappling with since the period proceeding Russia's illegal annexation of Crimea in 2014.[7] Some analysts also argue that Russia has refrained from using all of its capabilities to conduct large-scale cyberattacks against Ukraine, and Moscow has certainly learned lessons from its successes and failures on the cyber battlefield in Ukraine as well. Further, Russia's 2021 National Security Strategy emphasizes using advanced technologies such as artificial intelligence (AI) and quantum computing as multipliers for its cyber capabilities.[8] Now, and increasingly as these capabilities come online, Russian cyber operations pose a serious threat to the United States and its allies.

Russia's war against Ukraine is a unique case that could provide false reassurance that a cyber conflict between Moscow and the United States would be inconsequential. That hope would be misplaced.

Core Elements of Russia's Strategy

Russia notably does not use the terms "cyber" (*kiber*) or "cyber warfare" (*kibervoyna*) when referring to its actions in cyberspace. Rather, Russia uses these terms only when talking about Western threats and activities. To describe its own activities, Russia uses the term "information confrontation," or IPb, which the Russian Ministry of Defence's Military Encyclopedia defines as "the clash of national interests and ideas, where superiority is sought by targeting the adversary's information infrastructure while protecting its own objects from similar influence."[9]

IPb covers a much broader range of activities than Western conceptions of cyber conflict. Importantly, it is not limited to wartime but rather is carried out continuously. The 2016 Doctrine of Information Security of the Russian Federation defines this domain as

> a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet . . . communications networks, information technologies, [and] entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere.[10]

In other words, Moscow views all elements of the cyber domain—governmental, personal, and corporate—as potential assets (or threats to its security) in a conflict. Due to the breadth of activities included, Russian military scholars divide IPb into two main subcategories: informational-technical confrontation and informational-psychological confrontation. The informational-technological aspect is largely comparable to Western conceptions of cyber warfare and involves attempts to attack and gain access, disrupt, or damage enemy computers or information networks. This aspect

includes cyber espionage, malware, denial-of-service (DoS) attacks, distributed-denial-of-service (DDoS) attacks, and supply chain attacks.[11]

Moscow views all elements of the cyber domain—governmental, personal, and corporate—as potential assets (or threats to its security) in a conflict.

Informational-psychological confrontation has no single parallel concept in Western cyber doctrine. The Russian Ministry of Defence's Military Encyclopedia defines it as influencing "the enemy's information resources, the consciousness and feelings of their military personnel and population, as well as a set of measures to protect one's own information and psychological resources."[12] It includes efforts to influence an enemy's population and military forces by shaping the enemy's perceptions and manipulating their thoughts and behavior. The eventual goal of informational-psychological confrontation might be to force the enemy population to support the aggressor or to "prolong internal deliberations on policy decisions within the adversary state."[13] Russia's activity in this space has broad implications for the West since the United States and its allies value free speech highly and have been slow to recognize this as an area of vulnerability. In the remainder of this chapter, the terms "IPb," "information warfare," and "information doctrine" encompass both informational-technical and informational-psychological confrontation and reflect Russian thinking on the subject, though most of the focus will be on informational-technical warfare. (For more on informational-psychological confrontation, see the appendix.)

How Cyber Strategy Fits into Foreign Policy

Russia views IPb as both a means of achieving its strategic and political objectives and as a threat emanating from the West. The Kremlin's actions are shaped by a belief that it is already in an information war with the United States and its allies. As former Russian Defense Minister Sergei Shoigu highlighted, Moscow believes "Western countries, led by the United States, have unleashed an absolutely unprincipled information war against Russia."[14] As a result, Russia's defining approach to information warfare could be described as adhering to the adage "the best defense is a good offense," combined with a near-paranoid view of the need to protect the domestic information space.

Because Moscow portrays itself as constantly under attack from the West, it describes its information strategy as entirely defensively oriented. A 2022 study by the RAND Corporation shows that Russia's "doctrinal publications omit offensive actions, instead emphasizing defensive and collaborative measures, even legal frameworks and partnerships to prevent aggression."[15] Russia's 2016 Information Security Doctrine clearly reflects this focus on a pervasive threat and defensive measures: "Intelligence services of certain States are increasingly using information and psychological tools with a view of destabilizing the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of other States."[16]

Russia's defining approach to information warfare could be described as adhering to the adage 'the best defense is a good offense,' combined with a near-paranoid view of the need to protect the domestic information space.

As a result of the perceived threat emanating from the West, Moscow emphasizes the need to protect its domestic information environment and ensure what Russia refers to as "digital sovereignty." Following a series of events—including the Arab Spring uprisings, protests against Russian President Vladimir Putin in 2011 and 2012, and the Edward Snowden leaks in 2013—Moscow's fear of the internet and Western online interference accelerated. As a result, Russia began to take steps to tighten its grip on the Russian-language information space, dubbed RuNet. In 2012, the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) started maintaining a centralized internet blacklist, which Russian internet service providers use to manage Russia's firewall. The blacklist covers territories where Russia has a significant presence, such as Belarus and all Russian-occupied territories, like eastern Ukraine.[17] Since then, the Russian government's tactics to isolate the internet within Russia have grown increasingly aggressive and have included blocking foreign media.[18]

Russia also uses IPb to further its strategic goals during peacetime. According to the 2010 Military Doctrine of the Russian Federation, a key feature of modern military conflict is the "prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force."[19] The Kremlin thus views IPb as a tool that can and should be used against countries not engaged in a direct armed conflict with Moscow. For example, Russian government actors hit Montenegro with a series of cyberattacks in 2016 and 2017 as Montenegro drifted away from Moscow—its former ally—and voted to join NATO. The 2016 attack targeted state digital infrastructure on election day, while the 2017 attack was a direct response to Montenegro joining NATO.[20] Since that time, Moscow has continuously "used cyberattacks . . . to redirect Podgorica toward its influence," including a massive attack in 2022 that crippled state-run transportation services and water and electricity systems.[21]

Similarly, Moscow uses IPb to raise fear and stoke instability in enemy populations. These cyber actions remain below the threshold of acts of war, which minimizes retaliatory responses, particularly from Western countries that do not have similar conceptions of cyber and information warfare and the use of these tools during peacetime.[22] For instance, in 2017, a spear-phishing campaign attributed to the Russian government targeted French President Emmanuel Macron's campaign team. Moscow stole and leaked gigabytes of data, but the Russian campaign was unsuccessful in that it did not affect the election results or antagonize French society. Nevertheless, the attack is a clear example of Moscow attempting to sow doubt in the electoral process and raise questions about France's stability.[23]

Further, Moscow believes IPb can be a tool to prevent armed confrontation. According to a NATO Defense College report, "Senior Russian officers have suggested that information effects . . . can in

some cases replace armed intervention altogether."[24] Russian conceptions of "strategic deterrence" (*sderzhivanie strategichesko*) also highlight this concept. The Russian Ministry of Defence's Military Encyclopedia defines strategic deterrence as "a coordinated system of forceful and non-forceful measures taken consecutively or simultaneously by one side in relation to another to keep the latter from any military actions that inflict or may inflict damage on the former on a strategic scale."[25] While not explicitly stated, IPb certainly falls under nonmilitary interventions and is therefore an important tool to prevent armed confrontation, especially in Moscow's strategy toward adversaries with stronger conventional capabilities, such as the United States and other NATO partners.[26]

Additionally, as seen in Russia's cyber operations in Ukraine and Georgia, IPb plays a critical role in Moscow's strategy during a kinetic conflict. Disabling critical infrastructure such as energy, transport, and command and control "can dramatically weaken an adversary's fighting capabilities" and thus help bridge the gap between Moscow's capabilities and the capabilities of its adversaries.[27] These cyber operations also have a psychological component aimed at keeping the adversary government distracted and affecting the psyche of the enemy population.[28]

These cyber operations also have a psychological component aimed at keeping the adversary government distracted and affecting the psyche of the enemy population.

The 2008 war between Russia and Georgia is often cited as the first time that a nation used cyber operations in tandem with military action. In August 2008, Russian troops invaded Georgia. Weeks before the kinetic conflict began, Russian hackers launched a "rehearsal" DDoS attack that took down numerous government websites, such as that of the Georgian president, for almost 24 hours.[29] Following the invasion, Russian hackers continued their attacks on an expanded list of targets in Georgia, including additional government sites, financial and educational institutions, and Western media sites such as CNN and BBC.[30] Georgian authorities blamed Russia broadly for the attacks, but Moscow denied the claims. The attacks have since been widely attributed to Russian hacktivist groups that are suspected to have coordinated closely with the government.[31]

The speed of the cyberattacks in Georgia suggests that reconnaissance took place well in advance of the attacks and the invasion. Cyber forces were prepositioned before the outbreak of kinetic conflict, meaning cyber actors had some degree of advanced planning.[32] The attacks also carefully avoided targets that would cause physical damage, despite likely having access to supervisory control and data acquisition (SCADA) systems that could have damaged critical infrastructure; this demonstrates that the Kremlin is selective about the accesses it chooses to exploit.[33]

Since 2008, Russia has continued to combine cyber operations with military action. For instance, the lead-up and period immediately following Russia's illegal annexation of Crimea in 2014 saw sustained cyberattacks. Russian threat actors conducted widespread cyber espionage on a series of Ukrainian targets and DDoS attacks against government websites and media, and the Kremlin

continued its cyberattacks against Ukraine "in parallel with protracted military confrontation in the Donbas." Similarly, Russia used cyber operations to support its 2022 full-scale invasion of Ukraine.[34] (For more information about cyber operations in parallel with Russia's full-scale invasion of Ukraine, see the case study on page 27.)

Cyber forces were prepositioned before the outbreak of kinetic conflict, meaning cyber actors had some degree of advanced planning.

How Russia Approaches Deniability

Russia's activities in cyberspace are bifurcated between two genres: (1) operations intended to create high-profile effects while providing some deniability to Moscow, and (2) operations intended to remain clandestine while achieving long-dwell espionage effects or while prepositioning for future attacks.

The first category includes Russian operations that aim to cause immediate disruption. Cyberattacks such as the 2007 DoS attacks on Estonian critical infrastructure, the 2015 and 2016 attacks targeting the Ukrainian power grid, and the 2018 attack on the Winter Olympics, for example, purposefully drew immediate attention while somewhat hiding Moscow's hand.[35] Throughout this time, Russia's Main Intelligence Directorate (GRU) took on a more high-profile role in cyberattacks, bringing with it "'a culture of aggression and recklessness' and a 'high tolerance for operational risk' that was unusual in the cyber domain."[36] In the heat of kinetic conflict such as the current war in Ukraine, Moscow issues weak denials of its disruptive cyber activities.[37]

Russia also uses its vast and opaque network of nongovernmental cyber actors to maintain a level of plausible deniability. This category of actors includes cybercriminals, patriotic hackers, and proxy organizations and front companies, which all receive varying amounts of support from the Kremlin. Moscow has differing levels of control over these groups, making it difficult for policymakers to determine the government's true degree of involvement and calculate an appropriate response.[38]

Moscow has also engaged in sophisticated long-term clandestine campaigns. These types of operations tend to be aimed at espionage—creating a long-term, quiet presence that can consistently deliver intelligence—or at creating a penetration that could be weaponized later. Sometimes the same exploit can deliver both. For instance, the 2020 SolarWinds compromise went undetected for at least nine months. During that time, the Kremlin stole the data of thousands of individuals and multiple federal agencies.[39]

In another instance, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert in 2018 highlighting that Russian actors had been targeting government entities and critical infrastructure sectors since at least 2016. The victims included both staging and intended targets: Russian cyber actors gained initial access to the less secure networks of staging targets and then used them as "pivot points and malware repositories when targeting their final intended victims."[40]

After gaining access to the intended targets, Russian actors conducted reconnaissance operations, moved laterally, and gathered information about industrial control systems (ICSs) and SCADA systems.[41] These Russian cyber actors were "positioning themselves for a limited or widespread attack," according to Michael Carpenter, former deputy assistant secretary of defense.[42]

Implementation: Campaigns or Opportunism?

The Kremlin sets long-term strategic goals. Then, this "commander's intent" funnels into particular campaigns with clear objectives. However, the targets of cyber operations within these campaigns are largely opportunistic—chosen because they feature a combination of alignment with a Kremlin objective and a critical security vulnerability. For example, Putin's strategic intent is clearly to undermine democracy in NATO nations. Russia has staged campaigns with this intent during the 2017 French and Dutch elections, both of which featured a far-right antiestablishment candidate likely to cause intense controversy.[43] These opportunities are fragile, momentary alignments where a useful target has a security flaw. Attacking those opportunities are operators from intelligence agencies, military units, arms-length contractors, and criminal groups temporarily pressed into service.

Attacks in Ukraine by different Russian threat actors have exemplified the same pattern. During the few weeks before and immediately following Russia's invasion, Moscow conducted a campaign to disrupt command and control infrastructure, interfere with banking, take over social media accounts, and spread fake news. However, after this initial campaign culminated and energy shifted to kinetic warfare, cyber activity waned dramatically. Russia seemed to pursue opportunistic goals over the next several months as it likely worked to refresh its cyber tool kit.[44]

Moscow is also known to partake in opportunistic attacks against its adversaries that appear to be one-off retaliatory efforts. For example, in April 2015, a state-affiliated threat group—almost certainly the GRU—shut down 12 French television networks. The hackers shut down broadcasting with destructive malware and hijacked the network's website and social media. They posted jihadist propaganda, posing as supporters of the Islamic State and calling themselves the Cyber Caliphate.[45] The attack began in January 2015, two months after the French government canceled the sale of two warships to Russia in protest over Russian aggression toward Ukraine. While the reason for the attack has not been definitively established, it appears to have been opportunistic—likely a statement of revenge—rather than part of a larger campaign.[46]

Screenshot of TV5Monde's Facebook page following the Russian cyber attack.

Source: "France's TV5Monde targeted in 'IS group cyberattack'," France24, April 9, 2015, https://www.france24.com/en/20150409-france-tv5monde-is-group-hacking.

In particular, DDoS attacks by hacktivist groups have been extremely opportunistic, not very sophisticated, and minimally damaging. (For more on hacktivist groups, see page 24). For example, in August 2022, Russian hacktivist group Killnet claimed responsibility for more than 200 DDoS attacks against institutions across Estonia. Estonian authorities said they repelled the attacks, and for the most part websites remained available "with some brief and minor exceptions."[47] These attacks, however, served a purpose. If a group successfully takes a government site down—even for just two minutes—it can take a screenshot and use its success to recruit talent. The attacks also work to affect the psyche of the target population and thus potentially help Russia's cause.[48]

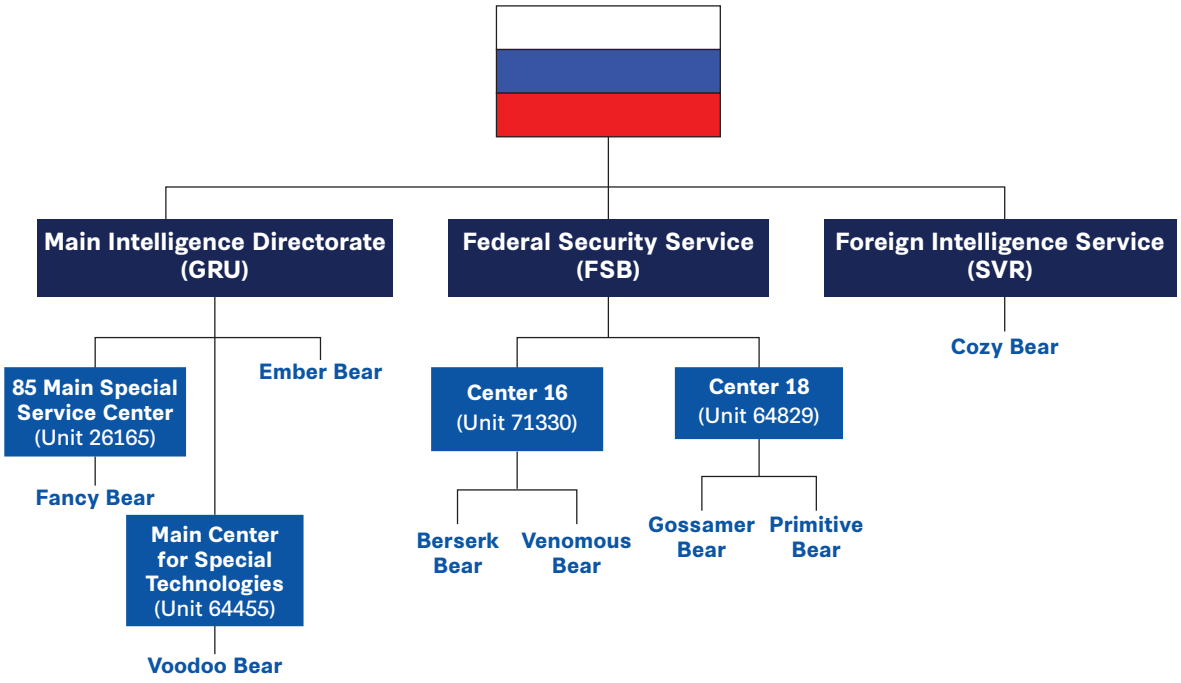
There are a few public instances of Moscow carrying out long-term, persistent presence operations as part of a sustained campaign. For instance, in December 2015, the Russian hacking group Voodoo Bear attacked Ukrainian power distribution companies and caused a power outage for more than 230,000 residents in western Ukraine.[49] This operation began as early as May 2014 with phishing emails and reconnaissance, through which Voodoo Bear was able to install the Trojan malware BlackEnergy 3 on utility companies' systems. Voodoo Bear also tried a series of methods to extend blackouts—for instance, by carrying out a DoS attack against one company's call center and tampering with equipment at another to slow recovery operations. This attack was carefully planned over a series of months, and it served as a learning opportunity for future attacks on the Ukrainian power grid.[50]

Organization of Capabilities

Who Are the Fighters?

Moscow capitalizes on a talented set of government security services and a cadre of ostensibly private citizens to further its foreign policy goals. In government, no single Russian security or intelligence agency has sole responsibility for cyber operations, and observers have noted that coordination between cyber units is weak. This structure "contributes to competition among the agencies for resources, personnel, and influence" and may be why the units sometimes conduct similar operations "without any apparent awareness of each other."[51] The GRU, Federal Security Service (FSB), and Foreign Intelligence Service (SVR) all have capable internal offensive cyber groups with varying levels of tradecraft.

Figure 1: Russian Offensive Cyber Actors



Source: CSIS research.

MAIN INTELLIGENCE DIRECTORATE (GRU)

The GRU is Russia's military intelligence agency and has orchestrated some of Russia's most notorious high-profile cyberattacks. The GRU has demonstrated a willingness to conduct brazen and aggressive operations and has not necessarily attempted to maintain operational security or secrecy. GRU units responsible for cyberattacks include Fancy Bear (GRU 85 Main Special Service Center Unit 26165), Voodoo Bear (GRU Main Center for Special Technologies Unit 74455), and Ember Bear (unit not public). GRU Unit 54777 (72nd Special Service Center, Foreign Information and Communication Service) is responsible for the GRU's psychological operations, which include disinformation and information operations.

Fancy Bear

Table 1: Aliases of Fancy Bear

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Fancy Bear	APT28	STRONTIUM	Forest Blizzard	Iron Twilight	Sofacy

Fancy Bear is generally given credit for a long list of high-profile government and government-adjacent hacks, including attacks on the German parliament in 2014; French television station TV5Monde, the White House, and NATO in 2015; the Democratic National Committee (DNC) in 2016; and the International Olympic Committee in 2018.[52] According to a 2017 special report by FireEye, Fancy Bear has "engaged in extensive operations in support of Russian strategic interests"

since at least 2007.[53] In December 2016, the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a joint analysis report that linked Fancy Bear to Russian civilian and military intelligence services, and the United States identified Fancy Bear in a 2018 indictment as GRU 85 Main Special Service Center (GTsSS), military unit 26165.[54]

Fancy Bear typically targets NATO countries, with particular emphasis on attacking foreign governments, defense and aerospace sectors, research and financial institutions, and global media outlets.[55] It is best known for using spear phishing to target individuals as well as registering domains that resemble those of legitimate organizations to establish phishing sites and harvest credentials.[56] The threat group has dedicated considerable time to developing and updating malware, including DownRange, Foozer, WinIDS, XAgent, and X-Tunnel, and it has been known to exploit zero-day vulnerabilities.[57] After compromising an organization, Fancy Bear steals data, which it eventually leaks to further Russian political interests.[58]

Fancy Bear is responsible for the following notable cyberattacks:

- Perhaps the most well-known Fancy Bear attack targeting the United States is the 2016 breaches of the DNC and the presidential campaign of Hillary Clinton. The group stole thousands of documents, including "internal strategy documents, fundraising data, opposition research, and emails from the work inboxes of DNC employees."[59] Shortly after the breach was announced, an online persona identifying itself as Guccifer 2.0 and claiming to be a Romanian hacker leaked documents and emails.[60]
- In September 2016, the World Anti-Doping Agency (WADA) confirmed that Fancy Bear had compromised its networks and obtained athlete medical data (see image below). The data specifically revealed drug test results and "therapeutic use exemptions," or situations in which WADA allows athletes to use banned substances to treat legitimate medical conditions. Some commentators viewed the incident as Russian retaliation for a WADA report that suggested Russia should be banned from the Rio Olympics for systematic doping of Russian athletes.[61]

Fancy Bear's website following hack of World Anti-Doping Agency, 2016.

Source: "What we know about Fancy Bears hack team," BBC News, September 2016, https://www.bbc.com/news/newsbeat-37374053.

Voodoo Bear

Table 2: Aliases of Voodoo Bear

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Voodoo Bear	APT44	IRIDIUM	Seashell Blizzard	Iron Viking	Sandworm

Voodoo Bear is responsible for some of Russia's most brazen and destructive cyberattacks. The group is best known for targeting critical infrastructure, including the energy, financial, and transportation systems sectors, and is responsible for the first confirmed cyber operation to successfully target a power grid and cause power outages. The group appears to disregard or ignore the unintended effects of its attacks, as seen in the NotPetya malware that caused over $10 billion of damage globally and affected more than 60 countries.[62]

Voodoo Bear has been active since at least 2009, and in October 2020, the U.S. Department of Justice (DOJ) indicted six officers operating under the GRU's Main Center for Special Technologies (GTsST) Unit 74455 for numerous attacks that cybersecurity researchers tied to Voodoo Bear. According to a DOJ press release about the indictment, the attacks were

> intended to support Russian government efforts to . . . destabilize: (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and (5) the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag.[63]

A 2022 CISA report confirmed that Voodoo Bear is GTsST Unit 74455.[64] The group is responsible for the following notable cyberattacks:

- In December 2015, Voodoo Bear hacked the power grid in two western oblasts in Ukraine, leaving over 200,000 people without electricity.[65] In 2016, the group attacked the grid in Kyiv, which left residents in the northern part of the capital without electricity.[66] In 2022, Voodoo Bear hackers again targeted the Ukrainian power grid, causing a temporary power outage utilizing a novel technique. The threat group first attacked the victim's operational technology then deployed a new variant of CADDYWIPER malware to the critical infrastructure organization's IT environment.[67]
- In June 2017, the NotPetya malware attack targeted MeDoc, a tax-processing service in Ukraine. The malware soon spread globally and caused significant damage to countries and businesses outside of Ukraine. In the United States, the attack shut down a pharmaceutical manufacturer and affected the medical record systems of dozens of hospitals.[68] The attack is estimated to have caused more than $10 billion in damage.[69]
- In February 2018, Voodoo Bear deployed a destructive malware known as Olympic Destroyer, which caused technology issues during the opening ceremony of the Olympics in South Korea. The attack disrupted internet access and telecasts, shut down the official website of the Olympics, prevented spectators from printing out reservations and attending the ceremony, and grounded broadcasters' drones.[70]

Ember Bear

Table 3: Aliases of Ember Bear

CrowdStrike	Mandiant	Microsoft (new)	Other
Ember Bear	UNC2589	Cadet Blizzard	FROZENVISTA

Ember Bear is a relatively new advanced persistent threat (APT) group that has been active since at least 2020. In a January 2021 blog post, Microsoft Threat Intelligence links Ember Bear to the GRU and asserts that Ember Bear is independent from Fancy Bear and Voodoo Bear.[71] While a March 2022 CrowdStrike blog post similarly confirms that Ember Bear is distinct from Fancy Bear and Voodoo Bear, it does not formally attribute the group to the GRU, although it notes that the group's "target profile, assessed intent, and their technical tactics, techniques, and procedures (TTPs) are consistent with other GRU cyber operations."[72]

Ember Bear mainly targets Ukraine, but it has also attacked entities in Europe, Latin America, Central Asia, and NATO member states that provide military aid to Ukraine. The group attacks government services, law enforcement, nongovernmental organizations (NGOs), emergency services, and information technology (IT) service providers, but according to Microsoft, the group's operations are "comparatively less prolific in both scale and scope to more established threat actors" such as Fancy Bear or Voodoo Bear.[73] After Ember Bear infiltrates networks—typically by exploiting vulnerabilities in web, Confluence, and Exchange servers—the threat group gathers data before engaging in disruptive actions.[74] For example, in January 2022, a month before Russia invaded Ukraine, Ember Bear deployed WhisperGate, a malware that overwrites master boot records, against Ukrainian

government organizations. Microsoft found data exfiltrated from these hacks on a Tor .onion site called Free Civilian.[75]

Information Operations Troops

Separate from the cyber operations units, Moscow has a host of troops engaged in information operations.[76] In a 2017 speech to the Russian parliament, Defense Minister Shoigu referenced the existence of the Information Operations Troops (Voyska Informatsionnykh Operatsiy, or VIO). Reports indicate that the VIO has an "emphasis on information assurance, counterpropaganda, and psychological operations—much less on technical efforts."[77] The VIO has an estimated 1,000 total troops across 12 to 14 units.

One such unit is GRU Unit 54777, also known as the 72nd Main Intelligence Information Center, which operates at the center of the Russian military's psychological warfare capacity. In 2021, the U.S. Department of the Treasury confirmed that the 72nd Main Intelligence Information Center is a unit in Russia's Information Operations Troops.[78] It also has several front organizations, financed through government grants and run covertly, that spread false conspiracy narratives and disinformation. The two best-known organizations are InfoRos and the Institute of the Russian Diaspora.[79]

According to Western intelligence officials, Unit 54777 has worked alongside GRU cyber units throughout their operations since at least 2014. Unit 54777 is known to complement "cyberattacks with digital information operations through proxies and front organizations."[80] For example, before the annexation of Crimea in 2014, Unit 54777 sent advisers to Russia's various military branches and split 80 specialists among five sections: mass media, teleradio broadcasts, psychological and information operations, editorial publications, and the Center for Foreign Military Information.[81] Similarly, Unit 54777 likely worked with Fancy Bear in the Cyber Caliphate operations to hijack U.S. Central Command's Twitter and take France's TV5Monde off the air in 2015.[82]

FEDERAL SECURITY SERVICE (FSB)

The FSB is Russia's primary domestic security agency responsible for counterterrorism, internal and border security, and information security. It also engages in foreign intelligence collection and offensive cyber operations. The FSB is tasked with protecting Russia's cyberspace and monitoring domestic criminal hackers, a task shared with the Ministry of Internal Affairs.[83] Both media reporting and DOJ indictments have documented the close relationship between the FSB and criminal and civilian hackers, who are reportedly used to bolster FSB cyber units. (For more on nongovermental hackers, see page 22).

Within the FSB, there are two primary centers responsible for information security and cyber operations. First, Center 16, which includes Berserk Bear and Venomous Bear, hosts most of the FSB's signals intelligence capabilities. Next, the Center for Information Security, or Center 18, which includes Primitive Bear, mainly oversees domestic operations (including all territories that the Kremlin claims as part of Russia, such as Ukraine) and security but also occasionally conducts foreign operations.[84]

Berserk Bear

Table 4: Aliases of Berserk Bear

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Berserk Bear	TEMP.Isotope (UNC809/ UNC2486)	BROMINE	Ghost Blizzard	Iron Liberty	Crouching Yeti, Dragonfly

Berserk Bear has been active since at least 2010. Both the U.S. and UK governments assess that Berserk Bear is almost certainly the FSB's Center 16, also known as Military Unit 71330.[85]

Berserk Bear's activity may be divided into two distinct periods. Initially referred to as Energetic Bear, the group's first phase of activity lasted until 2014. During this time, it targeted manufacturing, oil and gas, and electric utility entities across North America and Europe, using traditional phishing attacks, watering hole attacks, and supply chain intrusions for initial access. These operations typically led to deployment of custom malware, primarily Sysmain and Havex, combined with commodity penetration testing and tools.[86]

Following public disclosure of Berserk Bear's capabilities in 2014, cybersecurity researchers believe the group "stopped using its known tools and retired its infrastructure."[87] During the brief break, the behavioral characteristics of Berserk Bear's activity shifted, but "enough technical and other links [remained] to associate this activity with previous campaigns."[88] The Dragonfly 2.0 campaign, likely launched in 2015, uses phishing and strategic web compromise methodologies as well as watering hole attacks.[89] What sets Berserk Bear's attacks apart from those of other Russian APTs targeting critical infrastructure such as Voodoo Bear is that there is no evidence its attacks are disruptive in nature; it gains access to adversary systems and steals data but "despite ample opportunity never actually exploit[s] sensitive systems to attempt to cause a blackout, plant data-destructive malware, or deploy any other sort of cyberattack payload."[90] Berserk Bear seems to carry out only reconnaissance operations, but researchers worry that the information gathered could be used for more disruptive purposes in the future.[91]

The U.S. government and its allies have found evidence of Berserk Bear hacking a range of entities, but it is difficult to gauge the extent of their work and the actual threat it poses. There are some notable examples:

- Berserk Bear targeted U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors in a years-long campaign beginning in March 2016 or earlier. In 2018, CISA released a report detailing Berserk Bear's actions.[92]
- In 2020, investigators discovered evidence of Berserk Bear using supply chain attacks to target German companies in the energy, water, and power sectors. German authorities stated that the attacker's goal was to "steal information or even gain access to productive systems," but there was no evidence of a disruptive attack on any network.[93]

- In October 2020, the FBI and CISA warned that Berserk Bear had hacked multiple U.S. state, local, and tribal-level government and aviation networks. Due to the proximity of this hack to the November 2020 elections, the attack raised concerns that election data had been compromised, although the FBI and CISA did not find any evidence of this.[94]

Venomous Bear

Table 5: Aliases of Venomous Bear

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Venomous Bear	UNC4210	KRYPTON	Secret Blizzard	Iron Hunter	Turla, Snake

Venomous Bear has been active since 2004. In May 2023, the U.S. government formally attributed Venomous Bear to an unknown unit within Center 16 of the FSB.[95]

Venomous Bear mainly targets foreign governments and militaries and diplomatic organizations such as ministries of foreign affairs and embassies. Although it has targeted entities in at least 45 countries, it appears to focus largely on former Eastern Bloc countries.[96] More recently, the group's targets have expanded to include victims operating in multiple sectors, such as education and pharmaceutical companies.[97] The group is known for conducting watering hole and spear-phishing campaigns, creating fake software update files, and using satellite communication hijacking for command and control. Venomous Bear has been known to use a wide range of sophisticated and custom malware, including Snake, Agent.BTZ/ComRAT, Mosquito, and LightNeuron.[98]

Venomous Bear is responsible for the following notable cyberattacks:

- In 2008, the U.S. Department of Defense suffered what was then "the worst breach of U.S. military computers in history" when a flash drive containing malicious code was inserted into a military laptop at a base in the Middle East.[99] Agent.BTZ infected U.S. Central Command networks and had the "ability to scan computers for sensitive information and send data to a remote command and control server." It took 14 months to remove the malware from military networks.[100]
- In 2014, Kaspersky Lab analyzed a large cyber espionage campaign called Epic Turla. Venomous Bear hackers infected hundreds of computers in more than 45 countries, specifically targeting Europe and the Middle East. Affected entities included government institutions, embassies, research and pharmaceutical companies, and military and educational organizations.[101] Hackers used a multistage attack, starting with spear-phishing emails with Adobe PDF exploits and watering hole attacks. As attackers gained confidence, they upgraded to using sophisticated backdoors such as the Carbon/Cobra system. Upon infiltrating a system, the group often deployed a rootkit, a type of malware that permits the infiltrator to covertly command and control the infected system.[102]
- In 2017, Venomous Bear targeted invitees, guests, and nation-state participants of the G20 summit in Hamburg, Germany. The group used a back door named KopiLuwak, which is

"capable of exfiltrating data as well as downloading and triggering additional malware and executing arbitrary commands on the infected machine." The campaign used watering hole and spear-phishing emails posing as an invitation for the G20 summit for the Task Force on the Digital Economy.[103]

- In 2017, Venomous Bear made headlines when it used comments on Britney Spears's Instagram to store the location of its command and control server.[104] After deploying malware to compromise a system, attackers used command and control servers to send instructions and receive stolen data. When decoded, the nonsensical comment on Britney Spears's photo—reading "#2hot make loved to her, uupss #Hot #X"—contains the central server's address. Venomous Bear likely hid this malicious comment on Britney Spears's Instagram due to the large amount of likes and comments each post receives, making it more difficult to find.[105]

Gossamer Bear

Table 6: Aliases of Gossamer Bear

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Gossamer Bear	UNC4057	SEABORGIUM	Star Blizzard	Iron Frontier	Callisto

Gossamer Bear has been active since at least 2017. In December 2023, the U.S. government formally attributed Gossamer Bear to the the FSB Center for Information Security, also known as Center 18, military unit 64829.[106] In 2021, the Security Service of Ukraine publicly associated Gossamer Bear with Primitive Bear, but other cybersecurity companies and researchers do not support this link.[107]

Gossamer Bear is known to target NATO countries, particularly the United States and the United Kingdom, and occasionally other countries in the Baltic, Nordic, and Eastern European regions. Within these countries, Gossamer Bear focuses on think tanks, institutes of higher education, defense and intelligence consulting companies, and NGOs. Gossamer Bear has also shown a unique interest in targeting individuals—in particular, former intelligence officials, experts in Russian affairs, and Russian citizens abroad—with Microsoft reporting that 30 percent of the tracked activity related to this threat group was delivered to consumer email accounts.[108]

Gossamer Bear gathers intelligence on target individuals to identify legitimate contacts in the target's social network. Based on the information it gathers, Gossamer Bear registers new email accounts that match the aliases of impersonated individuals before sending an initial benign email. After establishing contact, the group then sends an email referencing an attachment that was not attached. When the target replies, the hackers send a malicious attachment. One way Gossamer Bear conducts reconnaissance on potential targets is by creating fake LinkedIn profiles. In addition, Gossamer Bear has been documented using an organizational approach to phishing.[109]

Once Gossamer Bear has stolen a target's credentials, the threat actor has been known to sign into the victim's email account and download emails and attachments, set up persistent data collection, or engage in conversation with specific people of interest.[110]

Gossamer Bear is responsible for the following notable cyberattacks:

- During the summer of 2022, Gossamer Bear targeted three U.S. nuclear research laboratories, including Brookhaven, Argonne, and Lawrence Livermore National Laboratories. The attacks appear to have been unsuccessful.[111] A U.S. Department of Energy spokesperson said they did not find "evidence of information being compromised."[112]
- In February 2023, Gossamer Bear gained access to the private email of Stewart McDonald, a member of the UK Parliament affiliated with the Scottish National Party. He wrote on Twitter, "Over the past couple of weeks. I have been dealing with a sophisticated and targeted spear phishing hack of my personal email account, and the personal email account belonging to one of my staff. These hacks are a criminal offence."[113]

Primitive Bear

Table 7: Aliases of Primitive Bear

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Primitive Bear	UNC530	ACTINIUM	Aqua Blizzard	Iron Tilden	Gamaredon

Primitive Bear is a Russian threat group that has been active since at least 2013. In November 2021, Ukraine publicly linked Primitive Bear to Center 18.[114] According to the Security Service of Ukraine, the group is likely operating out of Russia-occupied Crimea.[115]

Primitive Bear tends to target the Ukrainian government and defense sectors. According to a 2021 report by the Security Service of Ukraine, the group conducts "targeted cyberintelligence operations against state bodies of Ukraine, primarily security, defense and law enforcement agencies, in order to obtain intelligence information."[116] The group is known for using methods of social engineering, especially sending phishing emails containing malicious Microsoft Office document attachments to potential victims on behalf of state bodies, international organizations, and individuals. It is also known to exploit zero-day vulnerabilities. The 2021 report highlights that Primitive Bear has been responsible for over 5,000 attacks against more than 1,000 government systems since 2014.[117]

FOREIGN INTELLIGENCE SERVICE (SVR)

The SVR is Russia's civilian foreign intelligence service, "aimed at protecting the individual, society, and the state from external threats."[118] It collects foreign intelligence using human, signals, electronic, and cyber methods. The SVR, unlike the GRU and FSB, tends to operate with a high degree of secrecy to avoid detection. Most cyber operations that have been attributed to the SVR are aimed primarily at gathering intelligence, and the SVR is known to have a high degree of technical expertise and professionalism.[119] Cozy Bear is the only APT that has been officially attributed to the SVR.

Cozy Bear

Table 8: Aliases of Cozy Bear

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Cozy Bear	APT29	NOBELIUM	Midnight Blizzard	Iron Hemlock	The Dukes

Cozy Bear has been active since at least 2008.[120] In 2018, the Dutch General Intelligence and Security Service reported that it had hacked Cozy Bear's servers as well as a security camera in its office.[121] The Dutch service passed the information to U.S. intelligence services, which strongly suggested that the group is a component of the SVR. The U.S. and UK governments have since both publicly attributed Cozy Bear to the SVR.[122]

Cozy Bear is known to target government, foreign policy, and security-related organizations in the United States, United Kingdom, and other NATO member countries as well as post-Soviet states.[123] Cozy Bear has used several intrusion methods, including widespread emails designed to look like high-volume spam messages and targeted spear-phishing emails. In some cases, Cozy Bear has used compromised third-party networks to conduct attacks, including sending phishing emails purportedly from the U.S. Department of State and Harvard University's Faculty of Arts and Sciences.[124]

According to a report by F-Secure, this group uses a "smash-and-grab approach involving a fast but noisy break-in followed by the rapid collection and exfiltration of as much data as possible." If Cozy Bear determines the target to be particularly useful, it will switch the tool set and employ stealthier tactics "focused on persistent compromise and long-term intelligence gathering."[125] The group is especially adept at incrementally modifying its tactics as cybersecurity researchers publish information about its tool set and operations.[126]

Cozy Bear is responsible for the following notable cyberattacks:

- In the SolarWinds hack of September 2019, Cozy Bear used a supply chain attack to insert malicious code into the SolarWinds Orion System. By attacking this third-party software, Cozy Bear compromised the networks and systems of thousands of organizations, including government agencies such as the Departments of Homeland Security and State as well as large private companies such as Microsoft and FireEye.[127]
- In 2016, Cozy Bear hacked the DNC. The group is believed to have had access to the DNC's network for over a year, waiting quietly and gathering information. Eventually, it leaked over 20,000 emails on WikiLeaks.[128] Fancy Bear was also involved in this hack, although cybersecurity researchers believe the two worked independently and the attack was not coordinated.[129] (See the section on Fancy Bear on page 11 for more.)
- Throughout 2020, Cozy Bear targeted various organizations involved in Covid-19 vaccine research and development in Canada, the United Kingdom, and the United States with custom malware known as WellMess and WellMail. The goal of these attacks was likely to steal information and intellectual property and answer intelligence questions related to Covid-19.[130]

OTHER ACTORS

TEMP.Veles

TEMP.Veles (also known as Xenotime) is a Russian threat group that has targeted critical infrastructure, focusing specifically on U.S. energy sector organizations.[131] The U.S. government attributed TEMP.Veles to the Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), which is a research organization under Russia's Ministry of Defence. The group has developed destructive malware for targeting industrial control systems.[132]

In 2021, DOJ indicted a TsNIIKhM employee for conducting computer intrusions against U.S. energy sector organizations. This employee also accessed the systems of a foreign oil refinery and deployed Triton malware.[133]

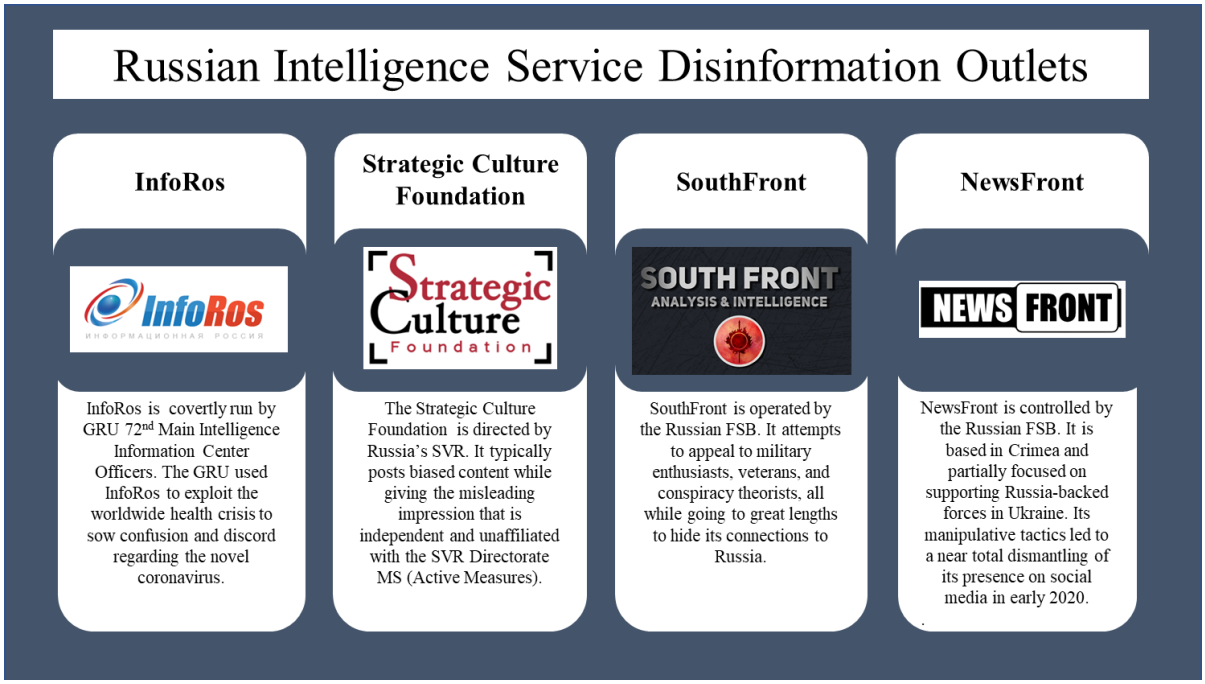
PROXY AND FRONT ORGANIZATIONS

The Russian government also finances and directs operations through front organizations and websites used to spread disinformation (see Figure 2). Proxy and front organizations allow Moscow to evade blame more easily by creating a veil of deniability. For example, the *Intelligence Community Assessment of Foreign Threats to the 2020 U.S. Federal Elections* highlights that Moscow "employed a system of government officials, disinformation outlets, and companies to covertly influence U.S. voters and spread misinformation."[134] Front companies included SouthFront, an online disinformation site that operates on behalf of the FSB; NewsFront, a Crimea-based disinformation and propaganda outlet that also worked with the FSB; the Strategic Culture Foundation, an online journal directed by the SVR and closely affiliated with the Russian Ministry of Foreign Affairs; and InfoRos, a so-called "news agency" run by the GRU's 72nd Main Intelligence Information Center (Unit 54777).[135]

Another notorious Russia-connected organization known for its disinformation campaigns is the Internet Research Agency (IRA). The IRA conducted propaganda and influence operations on behalf of Russian domestic, foreign policy, and business interests. In February 2023, Yevgeny Prigozhin, then head of the Russian private military company Wagner Group, admitted on a Wagner Telegram channel that he founded the IRA. Following the failed Wagner rebellion in July 2023, the IRA dissolved.[136]

The Russian government also has relationships with legitimate Russian IT companies for various reasons. Some companies—including Pasit, AO; Neobit; and Advanced System Technology—technically support government cyber and information operations. They act as covert contractors for the Kremlin and conduct research and development on behalf of the FSB, GRU, and SVR. Other companies, such as Positive Technologies (a Russian IT security firm), host large-scale conventions that are known recruiting events for the FSB and GRU.[137]

Figure 2: Russian Intelligence Service Disinformation Outlets



Source: U.S. Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," Press release, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0126.

NONGOVERNMENTAL ACTORS

Russia is home to a vast, complicated, and opaque network of nongovernmental cyber actors that receive varying amounts of support or instruction from the Kremlin. There is no central body that coordinates this network, which includes "cybercriminals who operate without state backing and inject money into the Russian economy, patriotic hackers and criminal groups recruited by the state on an ad hoc basis, and proxy organizations and front companies created solely to conduct government operations, providing the Kremlin a veil of deniability."[138]

The government's involvement and influence range from giving direct orders and financial support to simply permitting operations so long as the actor's operations do not counter the interests of the Putin regime. This means Moscow has varying levels of control over these actors.

The Russian government leans heavily on nongovernmental entities to further Moscow's foreign policy goals. Using cybercriminals makes it harder for adversaries to respond, as it adds uncertainty about attribution of the attack and thus the appropriate retaliation tactics. It is also a cheap way to accomplish Moscow's goals of disruption. Russia-based or Russian-sponsored groups rarely conduct operations inside Russia or against Russian allies; instead, they focus on the United States, Europe, and Western-allied nations such as Canada and Australia—a particularly striking pattern when looking at criminal groups.[139]

Using cybercriminals makes it harder for adversaries to respond, as it adds uncertainty about attribution of the attack and thus the appropriate retaliation tactics.

Cybercriminals

The Russian government allows financially motivated cybercrime groups to operate for a variety of reasons. Cybercrime brings money into Russia, and it also helps cultivate cyber talent, which the Kremlin can call on as needed. There is a mutual understanding between the Kremlin and these groups that they will be permitted to operate freely as long as they focus mainly on foreign targets, do not undermine Moscow's foreign policy goals, and are responsive to government requests.[140]

There are multiple examples of the Russian government recruiting criminal hackers, often through the FSB. This pattern was solidified during the 2008 Russo-Georgian war. A hacker told the Latvian news site Meduza that since the start of the conflict, Russian authorities "have regularly recruited hackers to work for them, sometimes voluntarily and sometimes under the threat of criminal prosecution."[141] Further, in 2017, DOJ charged two FSB officers and their criminal conspirators with "computer hacking, economic espionage, and other criminal offenses."[142] According to the press release, the two FSB officers "protected, directed, facilitated and paid criminal hackers to collect information through computer intrusions."[143] These groups include TeslaBotnet, NetSide, BLOODNET, and UserSec, among others. Table 9 provides details about a select number of Russian cybercriminal groups.

Table 9: Information about Select Russian Cybercriminal Groups

Group	Description
Evil Corp	Evil Corp is a Russia-based cybercriminal organization responsible for the development and distribution of the Dridex malware.[144] The FSB is known to cultivate and co-opt Evil Corp hackers, enabling them to engage in disruptive ransomware attacks and phishing campaigns.[145]
The CoomingProject	The CoomingProject is a criminal group that extorts money from victims by exposing or threatening to expose leaked data.[146] The group stated that it would support the Russian government in response to perceived cyberattacks against Russia.[147]
Wizard Spider (also known as Conti)	Wizard Spider is a cybercrime group that develops TrickBot and Conti ransomware.[148] Wizard Spider pledged support to the Russian government and has threatened critical infrastructure organizations in countries perceived to have carried out cyberattacks or war against the Russian government.[149] The pledge was later updated to include the threat of retaliation against perceived attacks against the Russian people.[150]

Hacktivists

Beyond directly recruiting criminal hackers, Moscow also uses patriotic hackers, or hacktivists, to carry out cyber operations on its behalf. These groups, which vary greatly in terms of size and level of organization, conduct cyber operations in line with what they perceive as the Kremlin's interests because they genuinely believe they are expressing patriotism for the Russian nation. Some cybercriminal groups have also expressed their support for Russia and the desire to back the Kremlin, particularly since Moscow's invasion of Ukraine.[151]

There is speculation regarding ties between patriotic hackers and the Russian government. Moscow does not attempt to hide its appreciation for their work. For example, in 2017, Putin bragged that Russian hacktivists "wake up in the morning, they read about some developments in international affairs, and if they have a patriotic mindset, then they try to make their own contribution the way they consider right into the fight against those who have bad things to say about Russia."[152] Some cybersecurity researchers have even assessed with moderate confidence that these groups at least coordinate with the GRU, SVR, and FSB. Table 10 shows a few notorious hacktivist groups.

Table 10: Information about Select Hacktivist Groups

Group	Description
Killnet	Killnet has been active since at least January 2022 and is known for its DDoS campaigns against countries supporting Ukraine, particularly since Russia's invasion of Ukraine in March 2022. Killnet released a video in March 2022 pledging support to Russia.[153]
XakNet Team	XakNet Team has been active since at least March 2022. The group claims to be composed of Russian patriotic volunteers and has likely been working or associated with Killnet.[154] Mandiant reported finding a technical artifact from a Fancy Bear intrusion in one XakNet data leak, indicating that Fancy Bear had access to the same parts of the network from which the leak was sourced. Mandiant assesses with moderate confidence that moderators behind XakNet Team are at least coordinating with the GRU.[155] They are also speculated to coordinate with Infoccentr and CyberArmyofRussia_Reborn.
NoName 057(16)	NoName 057(16) has been active since March 2022 and is known for its DDoS attacks on Ukrainian, U.S., and European government agency, media, and private company websites. According to cybersecurity firm Radware, the group's motivation is to silence anti-Russian information.[156] They are also known to act alone and not make alliances with other hacktivist groups.[157]

Group	Description
Infoccentr	Infoccentr has been active since March 4, 2023, when its Telegram channel was created. The group conducts pro-Russia information operations and fights against anti-Russia and pro-Ukraine media. Mandiant assessed with moderate confidence that Infoccentr is coordinating with Fancy Bear "due to the timing of the leaks and the group's connection to XakNet."[158]
CyberArmyofRussia_ Reborn	The CyberArmyofRussia_Reborn Telegram channel has been active since at least April 2022. This group has leaked data from victims in several industries, and they have claimed to degrade or deny services through DoS and DDoS attacks. Mandiant assesses with moderate confidence that CyberArmyofRussia_ Reborn is coordinating with Fancy Bear.[159]

Internal Rivalries

This large array of options means Moscow can tailor the tool to the mission. It can use a sliding scale of sophistication and closeness to the government. For sensitive missions that require stealth or persistence, it has a range of sophisticated and talented in-house operators. For less sensitive missions, where attribution directly to the Russian government would be escalatory or politically awkward, it can call upon myriad criminal groups at any time. Moscow's security services can recruit these criminal groups with an implied threat: either participate or be shut down. However, this calibration works only up to a point. Target nations are getting better at attribution, and some are willing to speak out publicly. An operation that is meant to be quiet can easily become loud, as in the case of SolarWinds.

Having several in-house cyber operators is not unusual. Most nations with a robust cyber capability have the same setup. In Russia, however, these services tend to compete rather than collaborate. Jockeying for the leader's favor is a continuing feature of Russian government infighting, and Putin gives or retracts his favor as he approves or disapproves of an operator's performance. That competition can lead to mistakes, but it also engenders aggressiveness and resilience. If one set of capabilities is disrupted, others exist to fill the void.

Case Study

Russia Targets Ukraine, Again

Ukraine has been a consistent target of Russian cyberattacks, particularly since the 2013 Maidan protest movement and the 2014 illegal annexation of Crimea. Since then, Moscow has continually gathered intelligence on Ukraine and conducted cyberattacks with varying levels of disruption. In support of Russia's long-term goal to control Ukraine, Russian attacks intensified in the weeks leading up to the full-scale invasion on February 24, 2022. At this time, Russian-affiliated actors went after a range of targets, with some attacks intended to cause immediate disruption and others intended to remain clandestine.

On January 14, 2022, Ukraine suffered the first major cyberattack in the series of attacks leading up to the invasion. The attack affected more than 70 government websites, including the country's treasury, the National Emergency Service, and several ministries, causing them to display a message saying, "Be afraid and expect the worst."[160] The attacks were disruptive but minimally damaging: the vast majority of the websites were recovered within days.[161] These types of cyber operations, however, have been an important part of Moscow's strategy, undertaken by both government actors and hacktivists. They aim to destabilize Ukrainian society by keeping the Ukrainian government distracted and by affecting the psyche of the Ukrainian population.

A month later, Ukraine's largest bank, PrivatBank, was hit by a DDoS attack that temporarily interfered with online banking transactions. The attack also disrupted the websites of Ukraine's Ministry of Defence and armed forces, and Russian-affiliated actors went after oil and gas companies, sparking fears of broader cyberattacks should the conflict escalate.[162] In the run-up to a war, these are exactly the aspects of society a belligerent actor intent on quickly subduing a population would seek to disrupt: trust in the military, the ability to withdraw money from banks,

Photo Source: Jorge Ferreiro/Adobe Stock

and access to fuel that would facilitate travel. If successfully executed, gutting these three sectors would prevent civilian mobility during crises and dampen hope. The public would become hostage, trapped in the line of fire.

Two days later, the U.S. government declassified information stating that Russian government hackers had penetrated Ukrainian military, energy, and other critical networks. The hackers, probably affiliated with the FSB and GRU, were lingering in the networks to collect information and position themselves to disrupt the systems in the wake of a full-scale invasion.[163]

When the conflict shifted from operational preparation of the environment to open war, Russia's efforts refocused on government targets, communication infrastructure, power, and media. Hours before the invasion in February, Russian actors, probably affiliated with the GRU, carried out a cyberattack that disrupted satellite communications in Ukraine, disconnecting thousands from the internet and potentially disrupting Ukraine's ability to communicate with its troops.[164] Some Ukrainians reported having no internet access for more than two weeks following the attack, and it even affected connectivity in France and Germany. The overall consequences, however, were not particularly severe, and Ukrainian military and intelligence officials said the attack had only a negligible operational impact.[165]

Cyberattacks have continued throughout the war. The GRU has been responsible for the majority of the disruptive cyberattacks in Ukraine, including on the power grid.[166] The FSB has also been involved in cyberattacks on Ukraine, particularly cyber espionage campaigns against political and military targets as well as government institutions.[167] Similarly, according to Microsoft, SVR-affiliated Cozy Bear has carried out espionage attacks against political parties and the military.[168] Finally,

Russian hacktivist groups such as Killnet, Anonymous Russia, and the People's Cyber Army significantly increased their activity in Ukraine following Russia's full-scale invasion.[169]

Russia's cyber operations in Ukraine, however, have failed to achieve their objectives. The apparent lack of disruption has not been from a lack of Russian effort. Rather, the lack of coordination between various actors has crippled Russian success. According to a report by the George C. Marshall European Center for Security Studies, the FSB, GRU, and SVR "compete more than they cooperate."[170] The three state agencies have a fierce rivalry that makes coordination and cooperation extremely unlikely. These tensions were further stoked soon after the full-scale invasion, when Putin removed the FSB from the Ukraine portfolio and put the GRU in charge, likely intensifying competition between the two and dampening any possibility for collaboration.[171] Cyberattacks have also been poorly coordinated with Russian military actions, partially attributable to the ongoing mistrust between agencies.[172]

Ukraine's strong defenses have further contributed to Russia's failure to cause disruption. Ukraine has suffered from Russian aggression in the cyber domain for years and is aware of the need for resilience. Kyiv has created redundant internet infrastructure, trained talented cyber defenders, and recruited allies in Western governments and technology companies. Amid Russia's invasion, professionals at Microsoft, Mandiant, and others have sat side by side (virtually and literally) with Ukrainian defenders, limiting damage and restoring critical systems.

Russia's war in Ukraine is a unique case, so it remains difficult to gauge the full extent of Russian capabilities and how Russia might engage with other states in a similar scenario. The *2023 Annual Threat Assessment of the U.S. Intelligence Community* highlights that although Russia's cyber activity has thus far fallen short of the expected impact, Russia remains "a top cyber threat as it refines and employs its espionage, influence, and attack capabilities," learning from its previous attacks.[173] Some analysts also argue that Russia has thus far refrained from using all of its capabilities and conducting large-scale cyberattacks against Ukraine. Additionally, Russia's 2021 National Security Strategy emphasizes Moscow's work toward using advanced technologies such as AI and quantum computing in its cyber capabilities, indicating that the Kremlin's tactics will continue to advance. The Kremlin therefore will continue to pose a serious threat to the United States and its allies.

Russia's cyber operations in Ukraine illustrate the key elements of Moscow's overall approach to warfare in the cyber domain. It has used a combination of government entities and hacktivist groups, still likely taking orders from Moscow, to execute its overall strategy. It has combined a strategic objective—undermining the Ukrainian government and disrupting normal state activities—with opportunistic attacks, striking where and when it can. Cyber activity switched from information warfare to a combination of information and disruptive warfare. The last point could be a sign of things to come, as Ukraine has often served as a test bed for Russian capabilities. Moscow has long had the ability to engage in cyber espionage and persistent access, but the 2022 invasion of Ukraine has shown the next level of warfare: pairing destructive and disruptive cyber activity with kinetic warfare.

About the Authors

Julia Dickson is a research associate with the Intelligence, National Security, and Technology Program at the Center for Strategic and International Studies (CSIS). Her research interests include cybersecurity and cybercrime and the role of technology in conflict. Prior to joining CSIS, she was awarded a Fulbright grant and spent a year teaching English in Osh, Kyrgyzstan. She was also previously a research assistant at the Wilson Center, an intern for the Conventional Defense Program at the Stimson Center, and a communications and outreach intern at the International Crisis Group. She holds a BA in international studies with a minor in French from the Johns Hopkins University.

Emily Harding is director of the Intelligence, National Security, and Technology (INT) Program and vice president of the Defense and Security Department at CSIS. As the head of the INT Program, she provides thought leadership on the most critical issues facing intelligence professionals and on the future of intelligence work. She also serves as vice president of the Defense and Security Department, where she is responsible for leading a team of world-renowned scholars providing policy solutions that shape national security. Drawing on her decades of experience in national security, Emily has established herself as an expert on how technology is revolutionizing national security work. Harding has served in a series of high-profile national security positions at critical moments. While serving as deputy staff director on the Senate Select Committee on Intelligence, she led the committee's investigation into Russian interference in the 2016 elections, which was lauded for its bipartisanship. At CIA, she led analysts and analytic programs through moments of crisis, including shepherding the Iraq Group during the attempted Islamic State takeover. During a tour at the National Security Council, she served as director for Iran. After leaving the White House,

her team ran the first Office of the Director of National Intelligence-led presidential transition, where she was responsible for briefing the incoming administration. Harding is an adjunct lecturer at the Johns Hopkins School of Advanced International Studies. Her analysis has appeared in the Wall Street Journal, BBC, NPR, Bloomberg, and other outlets. Harding holds a master's degree from Harvard University's Kennedy School of Government and a bachelor's degree from the University of Virginia.

Appendix A

Informational-Psychological Warfare

Although this part of the series focuses more on cyber operations than on psychological operations, Russian doctrine views the two as inseparable, and it is wise to at least attempt to see things from the viewpoint of one's adversary. While the main text focuses on cyber operations, this appendix delves deeper into these psychological concepts.

The Russian Ministry of Defence's Military Encyclopedia lists the following common techniques of informational-psychological confrontation:

- **Psychological pressure** seeks to "create emotional discomfort and neutralize a person's ability to think logically and rationally about the information provided to them." This method includes disinformation, manipulation of figures and facts, and biased selection of material.
- **Methods of unnoticed penetration into the consciousness of the enemy** involve "techniques aimed at gradual subconscious infection with the most attractive elements of the imposed way of life." This includes spreading values and culture through media, music, and fashion.
- **Techniques based on implicit suggestion and distortion of the laws of logic**, as the Military Encyclopedia states, are largely useful only on less educated portions of the population. They become less useful as the population becomes more aware. This method includes drawing conclusions without sufficient reason and making false analogies.[174]

As the Kremlin has realized it cannot compete directly with the West in conventional terms, Russian military doctrine has given these concepts an increasingly prominent role. Russia's understanding

Table A-1: Information Confrontation Subtypes

	Informational-psychological Confrontation	Informational-psychological Confrontation
Tools	▪ Active measures (*aktivnye meropriyatiya*) ▪ Reflexive control (*reflexivnoe upravlenie*) ▪ Military deception (*maskirovka*)	▪ DoS attacks, DDoS attacks, phishing attacks, ransomware, brute force attacks ▪ Electronic warfare
Key Targets	▪ Adversary civilian populations to undermine trust in leadership ▪ Adversary enemy leadership thought and decisionmaking processes	▪ Information and communications networks of government and military ▪ Critical infrastructure such as transportation or energy ▪ Media and social media
Examples	▪ Spreading disinformation and propaganda for psychological effects ▪ Exploiting enemy societal divides to cause disruption	▪ Destroying information and computer networks ▪ Obtaining unauthorized access to adversary networks

Source: Michelle Grisé et al., *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, August 2022), https://www.rand.org/pubs/research_reports/RRA198-8.html.

of the importance of information in conflict, however, has roots in Soviet-era practices. While Russian strategies are evolving to take advantage of technological change, Moscow's modern-day tactics continue to relate closely to Soviet theories, including **active measures** (*aktivnye meropriyatiya*), **reflexive control** (*reflexivnoe upravlenie*), and **military deception** (*maskirovka*).

The Soviet Union uses the term **active measures** to describe a range of covert and deniable political influence operations, including establishing front organizations, spreading disinformation, weakening confidence in leaders and institutions, disrupting relations between other nations, and orchestrating political unrest.[175] A key aspect of these campaigns includes "spreading disinformation among the population about the work of state bodies, undermining their authority, and discrediting administrative structures."[176]

Russian leaders see active measures as the most appropriate response to perceived threats from the West because they make use of Russian strengths to "exploit perceived Western weaknesses–from its divisions to its commitment to free speech and open politics."[177] For example, Russia actively seeks ways to exploit racial divides to subtly cause disruption. Ahead of the 2020 U.S. elections, the Russian government actively tried to stoke racial tensions, including attempting to incite white supremacist groups to violence. Similarly, around the 2016 elections, Russia sought to

increase domestic tension focused on issues of race by creating fake Black Lives Matter groups that advocated violence.[178]

Reflexive control involves manipulating an adversary's decisionmaking process in a way that is favorable for Russia. The Kremlin does so by altering the information space to affect adversary perceptions of the world, which neutralizes adversaries' strengths and causes them to choose the actions most favorable to Moscow. Actions within this category are not necessarily limited to influencing a single decision but can instead lead the adversary to "make a series of decisions that successively discard options that would improve their position, until they are finally faced with a choice between bad and worse, either of which options would favor Russia."[179] Reflexive control involves targeting decisionmaking factors through multiple vectors beyond spreading disinformation.

Finally, ***maskirovka***—translated as camouflage, concealment, or deception—has no equivalent in U.S. military doctrine but is a critical component of IPb. It is deeply rooted in Russian society and has long been an important component of Russian military operations. The primary purpose of *maskirovka* is to mislead an enemy regarding the disposition, composition, and intentions of its forces. It has evolved beyond Western ideas of military deception to a "broader set of means of denial and deception on a strategic level—including political, economic, and diplomatic measures to achieve international goals."[180]

At the same time as Moscow pursues these offensive tactics, it seeks to build its garden walls higher at home. Russia sees this push for digital sovereignty and having a closed RuNet as offering considerable advantages to its IPb strategy. The control of information makes Russia more resilient to information attacks and allows Moscow to maintain and extend its influence to Russian-speaking minorities abroad. According to NATO's Strategic Communications Centre of Excellence, Russia uses information control to gain "in terms of its societal resilience and recovery, integrity of command, and overall performance in times of mobilization." Conflict in the information space between Russia and its adversaries is therefore very asymmetric because "states operating within open networks would face a considerably constrained operating environment, whereas Russia, as a closed-network nation, would be able to operate with comparative freedom."[181]

In 2019, Putin signed the sovereign internet law, which requires internet providers to install "Deep Packet Inspection (DPI) equipment to auto-block banned websites, monitor cross-border communication, and allow Roskomnadzor to take the reins 'at a time of crisis'—a vaguely defined phrase."[182] This gives Roskomnadzor a high level of control over information flows in the Russian Federation, essentially allowing the country to isolate RuNet from the global internet at its own discretion.

Moscow assumes the West is engaging in a commensurate information war to diminish Russia's influence in the global information sphere and thus harm its international standing. In Russia's 2021 National Security Strategy, the Kremlin expresses its belief that adversary states are carrying out information campaigns to "form a hostile image of Russia."[183] The 2023 Concept of the Foreign Policy of the Russian Federation likewise lists one of its main foreign policy objectives in the

information sphere: countering "the coordinated anti-Russian propaganda campaign carried out on a systematic basis by unfriendly states."[184]

Moscow also uses information-psychological tools as a means of achieving its strategic objectives. The Kremlin recognizes the tactical importance of promoting a strong identity, so Russia's information operations are strongly associated with the country's desire to protect its sociocultural identity and promote the Russian language, which, according to Russia's 2016 Information Security Doctrine, is threatened by adversary states. Adversary states are exerting a "growing information pressure on the population of Russia . . . with the aim to erode Russian traditional spiritual and moral values."[185] In essence, Moscow seeks to create and maintain an alternative narrative to the English-language perspectives of the West. By villainizing the United States and its allies and creating a unified pro-Russia media space, Russia is attempting to counterbalance the global information space and create a medium through which it can spread its perspectives on global affairs. Such actions allow Moscow to advance the country's political, diplomatic, economic, and legal capabilities.

Endnotes

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

2 For the purposes of this paper, cyber operations are defined as actions that affect the 1s and 0s, meaning they change code to have a disruptive or destructive effect. By contrast, information operations use existing communication mechanisms to affect how people think about an issue or a situation. Rather than alter code, information operations take advantage of code as written to spread a message. A cyber operation may also have an information effect—for example, an operation to deface a website and install a hacking group's logo and message—but because it changes the existing website's code, it remains in the category of a cyber operation. Although information operations are, in a sense, agnostic to the vehicle for transmitting the message, vehicles such as social media have proved highly effective at pushing messages quickly and at scale.

3 Ellen Nakashima and Alex Horton, "Russian Hackers Have Probably Penetrated Critical Ukraine Computer Networks, U.S. Says," *Washington Post*, February 15, 2022, https://www.washingtonpost.com/national-security/2022/02/15/russia-ukraine-cyber-attacks/.

4 Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Endowment for International Peace, December 16, 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

5 Interview with Estonia's Information System Authority (RIA), September 26, 2023.

6 David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled into Ukraine, So Did Malware. Then Microsoft Entered the War," *New York Times*, February 28, 2022, https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html; and Ken Proska et al., "Sandworm Disrupts Power in Ukraine

Using a Novel Attack against Operational Technology," Google Cloud, November 9, 2023, https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology.

7 Microsoft, *Microsoft Digital Defense Report 2023* (Redmond, WA: October 2023), https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

8 Office of the President of the Russian Federation, *On the National Security Strategy of the Russian Federation* (Moscow: Kremlin, July 2021), https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf.

9 "Информационное противоборство" [Information confrontation], *Военный электронный словарь* [Military Electronic Dictionary], Министерство обороны Российской Федерации [Ministry of Defence of the Russian Federation], n.d., https://xn--d1abichgllj9dyd8a.xn--90anlfbebar6i.xn--p1ai/encyclopedia/dictionary/details_rvsn.htm?id=5221@@morfDictionary.

10 "Doctrine of Information Security of the Russian Federation," Совет Безопасности Российской Федерации [Security Council of the Russian Federation], December 5, 2016, http://www.scrf.gov.ru/security/information/DIB_engl/.

11 Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," *2020 12th International Conference on Cyber Conflict (CyCon)*, May 26–29, 2020, https://ieeexplore.ieee.org/document/9131723.

12 "Информационно-психологическое противостояние" [Information and psychological confrontation], *Военный электронный словарь* [Military Electronic Dictionary], Министерство обороны Российской Федерации [Ministry of Defence of the Russian Federation], https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=13183@@morfDictionary.

13 Michelle Grisé et al., *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, August 2022), https://www.rand.org/pubs/research_reports/RRA198-8.html.

14 "Defense Chief Says Western Countries Unleashed Unprincipled Information War against Russia," TASS Russian News Agency, March 7, 2023, https://tass.com/defense/1585727.

15 Grisé et al., *Rivalry in the Information Sphere*.

16 "Doctrine of Information Security of the Russian Federation," Совет Безопасности Российской Федерации [Security Council of the Russian Federation], December 5, 2016, http://www.scrf.gov.ru/security/information/DIB_engl/.

17 "Unified Register of the Domain Names, Website References and Network Addresses That Allow Identifying Websites Containing Information Circulation of Which Is Forbidden in the Russian Federation," Federal Service for Supervision of Communications, Information Technology, and Mass Media, accessed October 3, 2023, https://eais.rkn.gov.ru/en/.

18 Justin Sherman, "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior," Atlantic Council, July 12, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/.

19 President of the Russian Federation, "The Military Doctrine of the Russian Federation," translated by Carnegie Endowment for International Peace, February 5, 2010, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

20 "Montenegro's State Infrastructure Hit by Cyber Attack–Officials," Reuters, August 26, 2022, https://www.reuters.com/world/europe/montenegros-state-infrastructure-hit-by-cyber-attack-officials-2022-08-26/.

21 Julia Dickson and Emily Harding, "Russia Aims at Montenegro," CSIS, *Commentary*, February 13, 2024, https://www.csis.org/analysis/russia-aims-montenegro.

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

23 Heather A. Conley and Jean-Baptiste Jeangène Vilmer, "Successfully Countering Russian Electoral Interference," CSIS, CSIS Briefs, June 21, 2018, https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

24 Giles, *Handbook of Russian Information Warfare*.

25 "Сдерживание стратегическое" [Strategic deterrence], *Военный электронный словарь* [Military Electronic Dictionary], Министерство обороны Российской Федерации [Ministry of Defence of the Russian Federation], n.d., https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14206@@morf-Dictionary.

26 Ibid.

27 Hakala and Melnychuk, *Russia's Strategy in Cyberspace*.

28 Ibid.

29 Hakala and Melnychuk, *Russia's Strategy in Cyberspace*; and Andria Gotsiridze, "The Cyber Dimension of the 2008 Russia-Georgia War," *Rondeli Blog*, Georgian Foundation for Strategic and International Studies, September 8, 2019, https://gfsis.org.ge/cbgl/blog/view/970.

30 Paulo Shakarian, "The 2008 Russian Cyber Campaign against Georgia," *Military Review*, November-December 2011, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf.

31 David Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, January 6, 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

32 Shakarian, "The 2008 Russian Cyber Campaign."

33 Ibid.

34 Arnault Barichella, "Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe," Institut Jacques Delors, September 2022, https://institutdelors.eu/wp-content/uploads/dlm_uploads/2022/09/PP281_The-cybersecurity-dimension-of-the-war-in-Ukraine_Barichella_EN.pdf.

35 Josephine Wolff, "Understanding Russia's Cyber Strategy," Foreign Policy Research Institute, July 6, 2021, https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/.

36 Ibid.

37 Hakala and Melnychuk, *Russia's Strategy in Cyberspace*.

38 Justin Sherman, *Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior* (Washington, DC: Atlantic Council, September 2022), https://nsarchive.gwu.edu/media/29546/ocr.

39 "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response," *WatchBlog*, U.S. Government Accountability Office, April 22, 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

40 "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency (CISA), March 16, 2018, https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical.

41 Ibid.

42 Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *Wall Street Journal*, July 23, 2018, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110.

43 Conley and Vilmer, "Successfully Countering Russian Electoral Interference"; and Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace, May 23, 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

44 Interview with Estonia's Ministry of Defence, September 26, 2023.

45 Pierluigi Paganini, "The France TV5Monde Was Almost Destroyed by the Russian APT28 Group," Security Affairs, October 11, 2016, https://securityaffairs.com/52133/hacking/tv5monde-cyber-attack.html.

46 Gordon Corera, "How France's TV5 Was Almost Destroyed," BBC News, October 10, 2016, https://www.bbc.com/news/technology-37590375.

47 Andrius Sytas, "Estonia says it repelled major cyber attack after removing Soviet monuments," Reuters, August 18, 2022, https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/.

48 Interview with RIA, September 26, 2023.

49 "Compromise of a Power Grid in Eastern Ukraine," Council on Foreign Relations, December 2015, https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.

50 Donghui Park and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," Henry M. Jackson School of International Studies, University of Washington, October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

51 Andrew S. Bowen, "Russian Cyber Units," Congressional Research Service, February 2, 2022, IF11718, https://crsreports.congress.gov/product/pdf/IF/IF11718.

52 Cyware Hacker News, "Fancy Bear and Venomous Bear: What's the Difference between the Two Threat Groups?," Cyware Social, July 28, 2019, https://cyware.com/news/fancy-bear-and-venomous-bear-whats-the-difference-between-the-two-threat-groups-430d9985.

53 FireEye iSight Intelligence, *APT28: At the Center of the Storm* (Milpitas, CA: FireEye, January 2017), https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf.

54 National Cybersecurity and Communications Integration Center and Federal Bureau of Investigation, *Grizzly Steppe–Russian Malicious Cyber Activity* (Washington, DC: NCCIC and FBI, December 2016), https://www.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf; and National Security Agency et al., *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments* (Washington, DC: U.S. Department of Defense, July 2021), https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF.

55 "The Story of the Four Bears: Brief Analysis of APT Groups Linked to the Russian Government," Cybersecurity Help, January 17, 2022, https://www.cybersecurity-help.cz/blog/2507.html.

56 Editorial Team, "Who Is Fancy Bear (APT28)?," CrowdStrike, February 12, 2019, https://www.crowdstrike.com/blog/who-is-fancy-bear/.

57 "The Story of the Four Bears," Cybersecurity Help; and Pieter Arntz, "Fancy Bear Known to Be Exploiting Vulnerability in Cisco Routers," Malwarebytes Labs, April 20, 2023, https://www.malwarebytes.com/blog/news/2023/04/fancy-bear-known-to-be-exploiting-vulnerability-in-cisco-routers.

58 FireEye iSight Intelligence, *APT28*.

59 Editorial Team, "CrowdStrike's Work with the Democratic National Committee: Setting the Record Straight," CrowdStrike, June 5, 2020, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

60 FireEye iSight Intelligence, APT28.

61 Bill Chappell, "Russian Hackers Breached Athletes' Data, World Anti-doping Agency Says," NPR, September 13, 2016, https://www.npr.org/sections/thetwo-way/2016/09/13/493776953/russian-hackers-breached-athletes-data-world-anti-doping-agency-says.

62 "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, May 9, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a; and "3 Years After NotPetya, Many Organizations Still in Danger of Similar Attacks," Dark Reading, June 30, 2020, https://www.darkreading.com/threat-intelligence/3-years-after-notpetya-many-organizations-still-in-danger-of-similar-attacks.

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

64 "Russian State-Sponsored and Criminal Cyber Threats," CISA.

65 Donghui and Walstrom, "Cyberattack on Critical Infrastructure."

66 Pavel Polityuk, "Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid," Reuters, December 20, 2016, https://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF.

67 Patrick Howell O'Neill, "Russian Hackers Tried to Bring Down Ukraine's Power Grid to Help the Invasion," *MIT Technology Review*, April 12, 2022, https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/; and Ken Proska et al., "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology," Mandiant, November 9, 2023, https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology.

68 "Major Cyber Organizations of the Russian Intelligence Services," Department of Health and Human Services Office of Information Security, May 19, 2022, https://www.hhs.gov/sites/default/files/major-cyber-orgs-of-russian-intelligence-services.pdf.

69 Zaheer Merchant, "NotPetya: The Cyberattack That Shook the World," *Economic Times*, March 4, 2022, https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr.

70 Nicole Perlroth, "Cyberattack Caused Olympic Opening Ceremony Disruption," *New York Times*, February 12, 2018, https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html.

71 Microsoft Threat Intelligence, "Cadet Blizzard Emerges as a Novel and Distinct Russian Threat Actor," Microsoft Security Blog, Microsoft, June 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/.

72 CrowdStrike Threat Intel Team, "Who Is Ember Bear?," CrowdStrike, March 30, 2022, https://www.crowdstrike.com/blog/who-is-ember-bear/.

73 Microsoft Threat Intelligence, "Cadet Blizzard."

74 Ibid.

75 Ibid.

76 The focus of this report is cyber operations rather than information operations. It is, however, worth noting that Russia has a large Information Operations Troop because Moscow views information operations and cyberattacks as part of the broader concept of IPb, or information confrontation.

77 Gavin Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations," Carnegie Endowment for International Peace, December 12, 2022, https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

78 U.S. Department of the Treasury, "Treasury Escalates Sanctions against the Russian Government's Attempts to Influence U.S. Elections," Press release, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0126.

79 Council of the European Union, "Information Manipulation in Russia's War of Aggression against Ukraine: EU Lists Seven Individuals and Five Entities," Press release, July 28, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/.

80 Lilly and Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces."

81 Ibid.

82 Anton Troianovski and Ellen Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West," *Washington Post*, December 28, 2018, https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

83 "Federal Security Service," Government of the Russian Federation, http://archive.government.ru/eng/power/113/.

84 Bowen, "Russian Cyber Units."

85 "Russian State-Sponsored and Criminal Cyber Threats," CISA.

86 "Threat Profiles," Secureworks, accessed July 10, 2023, https://www.secureworks.com/research/threat-profiles/iron-liberty.

87 Ibid.

88 Joe Slowik, "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure" (paper presented at Virus Bulletin Conference, Wallingford, UK, October 2021), https://vblocalhost.com/conference/presentations/the-baffling-berserk-bear-a-decades-activity-targeting-critical-infrastructure/.

89 "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide," U.S. Department of Justice Office of Public Affairs, March 24, 2022, https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.

90 Andy Greenberg, "The Russian Hackers Playing 'Chekhov's Gun' with US Infrastructure," Wired, October 26, 2020, https://www.wired.com/story/berserk-bear-russia-infrastructure-hacking/.

91 "The Story of the Four Bears," CybersecurityHelp.

92 "Russian Government Cyber Activity," CISA.

93 Sean Lyngaas, "German Intelligence Agencies Warn of Russian Hacking Threats to Critical Infrastructure," CyberScoop, May 26, 2020, https://cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/.

94 "Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets," CISA, December 1, 2020, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-296a.

95 U.S. Attorney's Office for the Eastern District of New York, "Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service," Press release, May 9, 2023, https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network.

96 Matthieu Faou and Edward Millington, "Turla," Mitre Att&ck, last modified August 27, 2021, https://attack.mitre.org/versions/v10/groups/G0010/.

97 Ibid.

98 "Threat Profiles: Iron Hunter," Secureworks, https://www.secureworks.com/research/threat-profiles/iron-hunter.

99 William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, September 1, 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

100 "How Turla and 'Worst Breach of U.S. Military Computers in History' Are Connected," Kaspersky Lab, March 12, 2014, https://www.kaspersky.com/about/press-releases/2014_how-turla-and--worst-breach-of-u-s-military-computers-in-history-are-connected.

101 "Epic Turla," Targeted Cyberattacks Logbook, https://apt.securelist.com/apt/epic-turla.

102 Global Research and Analysis Team, "The Epic Turla Operation," Securelist, August 7, 2014, https://securelist.com/the-epic-turla-operation/65545/.

103 "Cyberespionage Group Turla Deploys Backdoor ahead of G20 Task Force Summit," Trend Micro, August 21, 2017, https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/cyberespionage-group-turla-deploys-backdoor-ahead-of-g20-summit.

104 Catalin Cimpanu, "Russian State Hackers Use Britney Spears Instagram Posts to Control Malware?," Bleeping Computer, June 6, 2017, https://www.bleepingcomputer.com/news/security/russian-state-hackers-use-britney-spears-instagram-posts-to-control-malware/.

105 Lindsay Maizland, "Britney Spears's Instagram is secretly being used by Russian hackers," Vox, June 8, 2017, https://www.vox.com/world/2017/6/8/15762122/russian-hackers-britney-spears-instagram.

106 U.S. Department of the Treasury, "United States and the United Kingdom Sanction Members of Russian State Intelligence-Sponsored Advanced Persistent Threat Group," Press release, December 7, 2023, https://home.treasury.gov/news/press-releases/jy1962; and "Gossamer Bear," Crowdstrike, n.d., https://www.crowdstrike.com/adversaries/gossamer-bear/.

107 Microsoft Threat Intelligence, "Disrupting SEABORGIUM's Ongoing Phishing Operations," *Microsoft Security Blog*, Microsoft, August 15, 2022, https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/.

108 Ibid.

109 "SEABORGIUM and TA453 Continue Their Respective Spear-Phishing Campaigns against Targets of Interest," National Cyber Security Centre, January 26, 2023, https://www.ncsc.gov.uk/news/spear-phishing-campaigns-targets-of-interest.

110 Ibid.

111 James Pearson and Christopher Bing, "Exclusive: Russian Hackers Targeted U.S. Nuclear Scientists," Reuters, January 6, 2023, https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06/.

112 Mark Harrington, "Reported Russian Cyberattack on BNL, Other Labs Appears Unsuccessful, Feds Say," *Newsday*, January 9, 2023, https://www.newsday.com/long-island/suffolk/brookhaven-national-lab-reuters-cyberattack-russians-j7s3f1c7.

113 Bill Goodwin, "Russian Hacking Group Seaborgium Targets SNP MP Stewart McDonald," ComputerWeekly.com, February 8, 2023, https://www.computerweekly.com/news/365530673/Russian-hacking-group-Seaborgium-targets-SNP-MP-Stewart-McDonald.

114 Gamaredon/Armageddon Group, *FSB RF Cyber Attacks against Ukraine* (Kyiv: Security Service of Ukraine, 2021), https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf.

115 Bowen, "Russian Cyber Units."

116 Gamaredon/Armageddon Group, *FSB RF Cyber Attacks*.

117 Ibid.

118 "Foreign Intelligence Service of the Russian Federation," Russian Government, n.d., http://government.ru/en/department/112/.

119 Bowen, "Russian Cyber Units."

120 "Threat Profiles: Iron Hemlock," Secureworks, n.d., https://www.secureworks.com/research/threat-profiles/iron-hemlock.

121 Eelco Bosch van Rosenthal, "Dutch Intelligence First to Alert U.S. about Russian Hack of Democratic Party," NOS, January 25, 2018, https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-us-about-russian-hack-of-democratic-party.

122 National Cyber Security Centre et al., *Advisory: Further TTPs Associated with SVR Cyber Actors* (London: Crown, May 2021), https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf.

123 "Threat Profiles: Iron Hemlock," Secureworks.

124 Ibid.

125 F-Secure, *The Dukes: 7 Years of Russian Espionage* (Helsinki: F-Secure, September 2015), https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf.

126 Ibid.

127 Saheed Oladimeji and Sean Michael Kerner, "SolarWinds Hack Explained: Everything You Need to Know," TechTarget, November 3, 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

128 Sam Thielman and Spencer Ackerman, "Cozy Bear and Fancy Bear: Did Russians Hack Democratic Party and If So, Why?," *The Guardian*, July 29, 2016, https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc.

129 Daniel Strauss, "Russian Government Hackers Broke into DNC Servers, Stole Trump Oppo," Politico, June 14, 2016, https://www.politico.com/story/2016/06/russian-government-hackers-broke-into-dnc-servers-stole-trump-oppo-224315.

130 National Cyber Security Centre et al., *Advisory: APT29 Targets COVID-19 Vaccine Development* (London: UK Government, July 16, 2020), https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF.

131 "TEMP.Veles," Mitre Att&ck, last modified October 17, 2021, https://attack.mitre.org/versions/v10/groups/G0088/.

132 "Russian State-Sponsored and Criminal Cyber Threats," CISA.

133 U.S. Department of the Treasury, "Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware," Press release, October 23, 2020, https://home.treasury.gov/news/press-releases/sm1162.

134 U.S. Department of the Treasury, "Treasury Escalates Sanctions."

135 Ibid.

136 "Russian Mercenary Chief Prigozhin Dead, Channel Affiliated with Wagner Says," Reuters, August 24, 2023, https://www.reuters.com/world/europe/russian-mercenary-chief-prigozhin-dead-channel-affiliated-with-wagner-says-2023-08-23/.

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

138 Sherman, *Untangling the Russian Web*.

139 Interview with RIA, September 26, 2023.

140 Sherman, *Untangling the Russian Web*.

141 Anna Shnygina, "'It's Our Time to Serve the Motherland': How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers," Meduza, August 7, 2018, https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

142 U.S. Department of Justice Office of Public Affairs, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," Press release, March 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

143 Ibid.

144 U.S. Department of the Treasury, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group behind Dridex Malware," Press release, December 5, 2019, https://home.treasury.gov/news/press-releases/sm845.

145 U.S. Department of the Treasury, "Treasury Sanctions Russia."

146 "Russian State-Sponsored and Criminal Cyber Threats," CISA.

147 "Here comes another one . . . Hello everyone this is a message we will help the Russian government if cyber attacks and conduct against Russia." ValeryMarchive, X post, February 25, 2022, 1:41 PM, https://twitter.com/ValeryMarchive/status/1497280612805324800.

148 "Russian State-Sponsored and Criminal Cyber Threats," CISA.

149 "The Conti #ransomware operation sides with Russia and threatens attacks on critical infrastructure." Brett Callow, X post, February 25, 2022, 10:36 AM, https://twitter.com/BrettCallow/status/1497249143663652865.

150 "Russian State-Sponsored and Criminal Cyber Threats," CISA.

151 Sherman, *Untangling the Russian Web*.

152 RFE/RL, "Putin Compares Hackers To 'Artists,' Says They Could Target Russia's Critics For 'Patriotic' Reasons," RadioFreeEurope/RadioLiberty, updated June 1, 2017, https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html.

153 CyberKnow, X post, March 3, 2022, 3:42 AM, https://x.com/Cyberknow20/status/1499349570890842113; and Mandiant Intelligence, "KillNet Showcases New Capabilities While Repeating Older Tactics," Mandiant, July 20, 2023, https://www.mandiant.com/resources/blog/killnet-new-capabilities-older-tactics.

154 "Russian State-Sponsored and Criminal Cyber Threats," CISA.

155 Mandiant Intelligence, "Hacktivists Collaborate with GRU-Sponsored APT28," Mandiant, last modified April 10, 2024, https://www.mandiant.com/resources/blog/gru-rise-telegram-minions.

156 "NoName057(16): Pro-Russian Hacktivist Group," Radware, n.d., https://www.radware.com/cyberpedia/ddos-attacks/noname057(16)/.

157 Daryna Antoniuk, "What's in a NoName? Researchers See a Lone-Wolf DDoS Group," The Record, September 4, 2023, https://therecord.media/noname-hacking-group-targets-ukraine-and-allies.

158 Mandiant Intelligence, "Hacktivists Collaborate with GRU-Sponsored APT28."

159 Ibid.

160 "'Be Afraid': Cyberattack in Ukraine Targets Government Websites?," Al Jazeera, January 14, 2022, https://www.aljazeera.com/news/2022/1/14/be-afraid-cyberattack-in-ukraine-targets-government-websites.

161 Sharon Rollins, "Defensive Cyber Warfare Lessons from Inside Ukraine," U.S. Naval Institute, *Proceedings*, vol. 49, no. 6, June 2023, https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine.

162 Ellen Nakashima and Alex Horton, "Russian Government Hackers Have Likely Penetrated Critical Ukrainian Computer Systems, U.S. Says," *Washington Post*, February 15, 2022, https://www.washingtonpost.com/national-security/2022/02/15/russia-ukraine-cyber-attacks/.

163 Ibid.

164 "Russian Cyberattack Takes Down Satellite Communications in Ukraine," German Marshall Fund of the United States, February 2022, https://securingdemocracy.gmfus.org/incident/russian-cyberattack-takes-down-satellite-communications-in-ukraine/.

165 "Case Study: Viasat," CyberPeace Institute, June 2022, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat; and Matthias Schulze and Mika Kerttunen, *Cyber Operations in Russia's War against Ukraine* (Berlin: Stiftung Wissenschaft und Politik, April 2023), SWP Comment 23, https://www.swp-berlin.org/10.18449/2023C23/.

166 Proska et al., "Sandworm Disrupts Power in Ukraine."

167 Kerstin Zettl-Schabath, Jakob Bund, Lena Rottinger, and Camille Borrett, *Gamaredon: Russian Intelligence Preparation of the Battlefield in Ukraine* (Heidelberg, Germany: European Repository of Cyber Incidents, January 2023), https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Gamaredon_13d3d3be46.pdf.

168 Daryna Antoniuk, "Kremlin-Backed Hacking Group Puts Fresh Emphasis on Stealing Credentials," The Record, June 21, 2023, https://therecord.media/nobelium-hacking-group-stealing-credentials/.

169 KELA Cyber Intelligence Center, "Russia-Ukraine War: Pro-Russian Hacktivist Activity Two Years On," *Times of Israel*, February 25, 2024, https://www.kelacyber.com/russia-ukraine-war-pro-russian-hacktivist-activity-two-years-on/.

170 Mark Galeotti, *The Intelligence and Security Services and Strategic Decision-Making* (Garmisch-Partenkirchen, Germany: George C. Marshall European Center for Security Studies, May 2019), https://www.marshallcenter.org/en/publications/security-insights/intelligence-and-security-services-and-strategic-decision-making-0.

171 Bill Bostock, "Putin Sacked the FSB and Put the Secretive GRU Spy Agency in Charge of Ukraine Intelligence after a String of Failures, Top Russian Journalists Say," Business Insider, May 10, 2022, https://www.businessinsider.com/putin-gru-in-charge-ukraine-intel-after-fsb-failures-report-2022-5.

172 Schulze and Kerttunen, "Cyber Operations in Russia's War against Ukraine."

173 "Russia Cyber Threat Overview and Advisories," CISA.

174 "Информационно-психологическое противоборств" [Information psychological confrontation], *Военный электронный словарь* [Military Electronic Dictionary], Министерство обороны Российской Федерации [Ministry of Defence of the Russian Federation], n.d., https://энциклопедия.минобороны.рф/encyclopedia/dictionary/details.htm?id=14727@@morfDictionary

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

176 Giles, *Handbook of Russian Information Warfare*.

177 Galeotti, *Active Measures*.

178 Julian E. Barnes and Adam Goldman, "Russia Trying to Stoke U.S. Racial Tensions before Election, Officials Say," *New York Times*, March 11, 2020, https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html.

179 Giles, *Handbook of Russian Information Warfare*.

180 Volodymyr Havrylov, "How Putin's Attempts at Deception Failed in Ukraine," Cipher Brief, November 15, 2017, https://www.thecipherbrief.com/column_article/putins-attempts-deception-failed-ukraine.

181 Hakala and Melnychuk, *Russia's Strategy*.

182 Emily Tavenner, "Russian Cyber Sovereignty: Global Implications of an Authoritarian RuNet," American University, February 1, 2022, https://www.american.edu/sis/centers/security-technology/russian-cyber-sovereignty.cfm.

183 Office of the President of the Russian Federation, *On the National Security Strategy of the Russian Federation* (Moscow: Kremlin, July 2021), https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf.

184 Office of the President of the Russian Federation, *The Concept of the Foreign Policy of the Russian Federation* (Moscow: Ministry of Foreign Affairs of the Russian Federation, March 2023), https://mid.ru/en/foreign_policy/fundamental_documents/1860586/.

185 "Doctrine of Information Security of the Russian Federation," Security Council of the Russian Federation.

COVER PHOTO LEENA MARTE/CSIS; MOCKO/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**