DFRLab

#ACcyber

CYBER STATECRAFT
INITIATIVE

ISSUE BRIEF

SEPTEMBER 2022

Untangling the Russian Web:
Spies, Proxies, and Spectrums of Russian Cyber Behavior

JUSTIN SHERMAN

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security

EXECUTIVE SUMMARY

The number of cyber operations launched from Russia over the last few years is astounding, ranging from the NotPetya malware attack that cost the global economy billions, to the SolarWinds espionage campaign against dozens of US government agencies and thousands of companies. Broad characterizations of these operations, such as "Russian cyberattack," obscure the very real and entangled web of cyber actors within Russia that receive varying degrees of support from, approval by, and involvement with the Russian government. This issue brief describes the large, complex, and often opaque network of cyber actors in Russia, from front companies to patriotic hackers to cybercriminals. It analyzes the range and ambiguity of the Russian government's involvement with the different actors in this cyber web, as well as the risks and benefits the Kremlin perceives or gets from leveraging actors in this group. The issue brief concludes with three takeaways and actions for policymakers in the United States, as well as in allied and partner countries: focus on understanding the incentive structure for the different actors in Russia's cyber web; specify the relationship any given Russian actor has or does not have with the state, and calibrate their responses accordingly; and examine these actors and activities from Moscow's perspective when designing policies and predicting the Kremlin's responses.

INTRODUCTION

The number of cyber operations launched from Russia over the last few years is astounding, ranging from the NotPetya malware attack that cost the global economy billions to the SolarWinds espionage campaign against dozens of US government agencies and thousands of companies. Yet broad characterizations of these operations, such as "Russian cyberattack," obscure the very real and entangled web of cyber actors within Russia that have varying degrees of support from, approval by, and involvement with the Russian government.

Contrary to popular belief, the Kremlin does not control every single cyber operation run out of Russia. Instead, the regime of President Vladimir Putin has to some extent inherited, and now actively cultivates, a complex web of Russian

cyber actors. This network 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 for the purpose of conducting government operations, providing the Kremlin a veil of deniability. This web of cyber actors is large, often opaque, and central to how the Russian government organizes and conducts cyber operations, as well as how it develops cyber capabilities and recruits cyber personnel.

Referring to all cyber activities that take place inside of Russia as "Russian"—and even those launched from outside Russia by "Russian" actors—flattens the complexity of this network and undermines analysis of the range of actors at the Kremlin's disposal. Likewise, assuming the Putin regime controls every single cyber activity emanating from Russia ignores the government's spectrum of involvement with various actors and, in turn, the different opportunities the United States and its allies and partners may have to disrupt Moscow's cultivation and use of this cyber ecosystem. While researchers continue to publish on the "cyber proxies" concept, proxy as a universal term fails to capture the gradations of the state's involvement with hackers, assuming a top-down hierarchical relationship that is not always present in Russia. Public information about this cyber ecosystem is not perfect or complete, but its relationship with the Russian government demands deeper analysis.

Untangling this multifaceted web—and understanding how and why so many Russian cyber actors freely operate in, and oscillate between, state and non-state domains—will allow the United States to appropriately target negotiations and track the expansion of Russian cyber operations globally. This is particularly important now, with the Putin regime facing an unprecedented level of sanctions from governments around the world, and the country's information technology (IT) "brain drain" accelerating since the regime's (re)invasion of Ukraine in February 2022.[1] Before these latest hostilities, the US government was negotiating a curtailment of ransomware attacks coming from within Russia; right after the war began, diplomatic talks between the Biden administration and the Kremlin quickly deteriorated.[2] Arguably, understanding and disrupting Russian cyber operations in conflicts in Ukraine and other areas around the world is more important than ever for the US government and its allies and partners. However, the reality is that the US government cannot pursue these objectives effectively or comprehensively without first understanding and shaping its approach around the reality of Russia's cyber ecosystem.

This four-part issue brief reviews the complex web of cyber actors in Russia, analyzes the range of Russian government involvement with these actors through specific examples, explains the risks and benefits the Kremlin perceives or gets from cultivating and leveraging this web of cyber actors, and provides three key takeaway-action pairings for US policymakers and its allies and partners.

A COMPLEX WEB: INHERITANCE MEETS CULTIVATION

Russia is home to a convoluted web of cyber actors comprised of government-funded front companies, state-tapped individuals, cybercriminals, and "patriotic hackers," among others. While some of these entities receive direct orders and financial support from Russian authorities, others have tacit permission to operate independently, so long as they do not upset the Putin regime. The Kremlin's involvement with each of these actors follows a varied and ambiguous pattern of engagement that the next section discusses in more detail. First, it is necessary to understand why the Russian government values this kind of cyberspace proxy activity, and how this activity has evolved into the convoluted and opaque web that exists in Russia today.

Political warfare is generally important to the Kremlin. The Putin regime, inside and beyond Russian borders, has carried out assassinations and attempted assassinations, funded propaganda front companies, spread disinformation, and launched disruptive cyber operations, among other activities. While the organizational structures that execute these activities, and the techniques used, vary, the goals are often similar: to disrupt, destroy, sabotage, and subvert enemies of the Russian state (read: enemies of the Putin regime) abroad and at home. This reflects a growing emphasis in Russia's military doctrine and national security thinking on the importance of information, proxy, and below-threshold-of-war conflict.[3] Russia's *2000 Foreign Policy Concept* stated that "while the [sic] military power still retains significance in relations among states, an ever greater role is being played by economic, political, scientific and technological, ecological, and information factors."[4] Prominent Russian military theorists S. G. Chekinov and S. A. Bogdanov underscored this in their 2010 article that appeared in the Russian journal *Military Thought*, writing that "asymmetric actions, too, will be used extensively to level off the enemy's superiority in an armed struggle by a combination of political, economic, information, technological, and ecological campaigns in the form of indirect actions and nonmilitary measures."[5] Some of these political warfare actions, like disruptive cyber

1 Dina Temple-Raston and Sean Powers, "'Cream of the Cream': Russia's High-Tech brain drain," *The Record*, May 10, 2022, https://therecord.media/cream-of-the-cream-russias-high-tech-brain-drain/.

2 See, for example: "U.S.–Moscow Ties Close to Rupture after Biden's 'War Criminal' Remarks, Russia Says," *Reuters*, March 21, 2022, https://www.reuters.com/world/russia-summons-us-envoy-says-ties-close-rupture-after-bidens-putin-comments-2022-03-21/.

3 See, for example: Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace* (Washington, DC: Georgetown University Press, 2019).

4 Russian Federation, *2000 Foreign Policy Concept of the Russian Federation*, June 2000.

5 S. G. Chekinov and S. A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought* (*Voyennaya Mysl'*), no. 3 (2010): 12–23, 16, https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf.

operations, explicitly target Russia's enemies, while others have intentional indirect effects. Scholars Adrian Hänni and Miguel Grossmann, for instance, argue that the Putin regime's "public, theatrical form of murderous attacks on intelligence defectors" is a kind of "signaling through covert action" to Russia's enemies, Russian defectors, and the Russian public.[6]

This assessment has its roots in historical actions, bureaucracy, and thinking that inform how Moscow uses cyber and information capabilities today. The Soviet Union conducted political warfare-style operations under an umbrella of "active measures" against foreign and domestic targets. Akin to contemporary political warfare, these actions ranged from assassinating *émigré* leaders who participated in anti-Soviet activities to manufacturing and spreading the lie that the Pentagon started the AIDS epidemic.[7] Of course, the parallels are not perfect, and the information environment today is fundamentally different than it was decades ago. For example, the scale and speed of microtargeting alone, enabled by the internet, is unprecedented. Regardless, the Putin regime and the Russian security apparatus continue to emphasize many of the same Soviet-era, active measures-type ideas, such as deniability, covertness, and the use of proxies, which carries over to cyber operations.[8] Russia's modern structure for information operations reportedly even mirrors the Soviet approach; after the collapse of the Soviet Union, the military transferred its propaganda directorate to the military intelligence agency (*Glavnoye Razvedyvatelnoye Upravlenie*, or GRU), rebranding it GRU Unit 54777 in 1994.[9] This unit still exists today and,[10] per the US Department of the Treasury's 2021 sanctions, falls under Russia's Information Operations Troops.[11] From strategic thinking to operational style to intelligence structure and culture, many similarities exist between the active measures of the Soviet Union and the political warfare activities of contemporary Russia.

To some extent the Putin regime inherited this convoluted web of cyber actors. Economic decline and political instability following the demise of the Soviet Union contributed to an explosion of crime,[12] including cybercriminal activity. Among other reasons, a lack of laws and enforcement related to cybercrime, limited economic opportunities, and "highly educated and technologically empowered segments of [the] population with the capability to conduct sophisticated criminal operations" all accelerated the pace of cybercrime in 1990s Russia.[13] This activity evolved from software piracy to more serious forms of profit generation like hacking banks and stealing identities.[14] By the time Putin ascended to the presidency in December 1999, there were already numerous nonstate hackers in Russia engaged in criminal behavior.

Instead of cracking down, the Kremlin actively cultivated this network of cyber actors, and continues to leverage this ecosystem for purposes that extend beyond criminal activity. The Putin regime allows cybercriminals and patriotic hackers to operate freely within Russia, so long as they focus on foreign targets, do not undermine the Kremlin's objectives, and answer to the state when asked. The Federal Security Service (FSB), Russia's internal security agency with some foreign purview, recruits cybercriminals to carry out operations on its behalf. The Foreign Intelligence Service (SVR) sets up front organizations to conduct cyber and information operations against foreign targets. The Kremlin permits private military companies (PMCs) to operate around the world and to sell their military and protective services to foreign governments; at least one Russian PMC has developed a cyber unit.[15] While Putin did inherit an ecosystem of both legitimate technology companies and technically talented individuals engaged in cybercrime, the regime has purposefully shaped this resource pool of Russian cyber actors to its own benefit, though not without accompanying risks.

It is worth noting that this issue brief focuses primarily on cyber operations as understood by the United States (pertaining to code) but also mentions information operations throughout (pertaining to, in the US view, human-readable content). Russia's conceptualization of the information space does not make such a firm distinction. Therefore, this

6 Adrian Hänni and Miguel Grossmann, "Death to Traitors? The Pursuit of Intelligence Defectors from the Soviet Union to the Putin Era," *Intelligence and National Security* 35, no. 3 (2020): 403–423, 404, 407.

7 See, for example: US Central Intelligence Agency, *Soviet Use of Assassination and Kidnapping*, Declassified, 1964, 1, https://carnegieendowment.org/files/SovietUseOfAssassination.pdf; Mark Kramer, "Lessons From Operation 'Denver,' the KGB's Massive AIDS Disinformation Campaign," *MIT Press Reader*, May 26, 2020, https://thereader.mitpress.mit.edu/operation-denver-kgb-aids-disinformation-campaign/.

8 Justin Sherman, "Digital Active Measures: Historical Roots of Contemporary Russian Cyber and Information Operations," *Georgetown Security Studies Review* 9, no. 2 (Washington, DC: Georgetown University's Edmund A. Walsh School of Foreign Service, April 2022): 1–9, https://georgetownsecuritystudiesreview.org/wp-content/uploads/2022/04/92_Final-1.pdf.

9 Andrei Soldatov and Michael Weiss, "Inside Russia's Secret Propaganda Unit," *Newsline Magazine*, December 7, 2020, https://newlinesmag.com/reportage/inside-russias-secret-propaganda-unit/.

10 See, for example: Antonin Toianovski 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.

11 To the reader, GRU Unit 54777 is also known as the 72nd Main Intelligence Information Center (GRITs), which the US Treasury Department identified as belonging to Russia's Information Operations Troops. US Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," April 15, 2021, https://home.treasury.gov/news/press-releases/jy0126.

12 See, for example: Mark Galeotti, "Gangster's Paradise: How Organized Crime Took Over Russia," *The Guardian*, March 23, 2018, https://www.theguardian.com/news/2018/mar/23/how-organised-crime-took-over-russia-vory-super-mafia; Vsevolod Sokolov, "From Guns to Briefcases: The Evolution of Russian Organized Crime," *World Policy Journal* 21, no. 1 (Spring 2004): 68–74, https://www.jstor.org/stable/40209904.

13 Dmitri Alperovitch and Keith Mularski, "Fighting Russian Cybercrime Mobsters: Report from the Trenches," BlackHat, July 25–30, 2009, 2, https://www.blackhat.com/presentations/bh-usa-09/ALPEROVITCH/BHUSA09-Alperovitch-RussCybercrime-PAPER.pdf.

14 Lucie Kadlecová, "Russian-Speaking Cyber Crime: Reasons Behind Its Success," *The European Review of Organized Crime* 2, no. 2 (2015): 104–121, 4, https://standinggroups.ecpr.eu/sgoc/russian-speaking-cyber-crime-reasons-behind-its-success/.

15 Emma Schroeder et. al, *Hackers, Hoodies, and Helmets: Technology and the Changing Face of Russian Private Military Contractors, Atlantic Council*, July 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/technology-change-and-the-changing-face-of-russian-private-military-contractors/, 5.

issue brief errs toward depicting the Russian understanding of the space, as well as highlighting some of the similarities between the ways Russian actors have conducted cyber and information operations, such as the government setting up cyber and information front organizations in other countries.

THE SPECTRUM OF RUSSIAN GOVERNMENT INVOLVEMENT

Putin does not control every single cyber operation that occurs within or comes out of Russia. In fact, as Candace Rondeaux writes, the "narrative of a grand chess master, whether Putin, a Kremlin insider, or a mercenary group, singlehandedly orchestrating Russia's proxy warfare strategy is a useful fiction for the Kremlin."[16] Simply put, "Vladimir Putin is not omnipotent," as journalist Julia Ioffe remarked in 2013.[17] In reality, there are degrees of Russian government involvement with most Russian cyber actors, whether it is through active financing, tacit approval, or another kind of engagement entirely. It is also possible that some activity is entrepreneurial by design, with nonstate hackers and developers auditioning their capabilities to capture the attention of the state.[18] Further, for all that Russian doctrines and military thinking emphasize the importance of political warfare and cyber and information operations, there is a great deal of complexity, competition, and internal conflict in how the Russian government bureaucracy attempts to operationalize those doctrines and ideas. Unpacking this spectrum of Russian government involvement with hackers is essential for the United States and its allies and partners to accurately analyze the Russian cyber web, as well as to identify areas to disrupt Russian government or government-directed activity.

In 2011, Jason Healey described a spectrum of state involvement in cyber activity,[19] identifying ten separate types of hacking: state-prohibited, state-prohibited-but-inadequate, state-ignored, state-encouraged, state-shaped, state-coordinated, state-ordered, state-rogue-conducted, state-executed, and state-integrated.[20] While Healey's intention was to enhance the conversation around government responsibility for cyber operations beyond technical attribution, his framework alone illustrates that governments can maintain a range of relationships with hackers to suit their purposes. Putin's regime has taken—and continues to take—this exact approach.

The extensive Russian network includes: internal government cyber and information units; front companies established and run by the government; private companies leveraged by the government to develop capabilities and recruit talent; criminals recruited by state officials; industry developers recruited by state officials; independently operating patriotic hackers (often with state encouragement or as cover for state-run action); hackers independently building their capabilities and pitching them to the state; and murky, mafia-style familial entanglements between hackers and Russian government officials. Experts have published excellent research on cyber proxies,[21] yet, in Russia's case, questions remain about the exact nature of those relationships, as they sometimes defy the frequent assumption that proxy activity refers to a top-down hierarchical relationship, with the state as the primary actor. Considerable portions of Russia's cybercriminal ecosystem operate with a sort of Darwinian entrepreneurialism, akin to the approach of Russian criminal enterprises and protective services in the 1990s.[22] Criminals often have substantial agency to drive this activity. And when there are quasi-symbiotic relationships at play with the state—a local FSB official, for instance, taking money on the side to provide a "roof" (*krysha*) of protection for hackers—these relationships do not entirely follow top-down or state-dominated definitions. It is also important to note, before diving into examples of actors in the Russian cyber web, that each case study raises questions about replicability.[23] Some examples may be entirely or somewhat replicable, while others could be one-off cases, shaped by factors such as the Russian government's operational needs, budgetary resources, technical constraints, and others.

The Russian government has many internal teams carrying out cyber operations. The FSB, GRU, and SVR all have cyber units, in addition to the cyber organizations located within other parts of the Russian military and security service apparatus.[24] For example, the FSB's 16th Center has signals intelligence capabilities, and its 18th Center has been respon-

16 Candace Rondeaux, *Decoding the Wagner Group: Analyzing the Role of Private Military Security Contractors in Russian Proxy Warfare, New America*, November 7, 2019, 8, https://www.newamerica.org/international-security/reports/decoding-wagner-group-analyzing-role-private-military-security-contractors-russian-proxy-warfare/.

17 Julia Ioffe, "Dear Lawrence O'Donnell, Don't Mansplain to Me About Russia," *The New Republic*, August 8, 2013, https://newrepublic.com/article/114234/lawrence-odonnell-yells-julia-ioffe-about-putin-and-snowden.

18 Thanks to Gavin Wilde for discussion of this point.

19 Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *The Brown Journal of World Affairs* 18, no. 1 (Fall/Winter 2011): 57–70, https://www.jstor.org/stable/24590776.

20 Jason Healey, *Beyond Attribution: Seeking National Responsibility in Cyberspace*, *Atlantic Council*, February 22, 2012, 2, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/.

21 See, for example: Healey, *Beyond Attribution*; Tim Maurer, *Cyber Mercenaries: The Stater, Hackers, and Power* (Cambridge: Cambridge University Press, 2017); Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?" *Orbis* 60, no. 3 (2016): 395–416.

22 Thanks to several individuals for discussion of this point. See, for example: Vadim Volkov, *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism* (Ithaca: Cornell University Press, 2002).

23 Thanks to a workshop participant for discussion of this point.

24 For a recently published discussion of the Russian government's cyber units, see: Andrei Soldatov and Irina Borogan, *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities* (Washington, D.C.: Center for European Policy Analysis, September 2022, https://cepa.org/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

sible for hacks of Yahoo, Ukrainian targets, and others.[25] The GRU has multiple cyber teams, including Unit 26165 ("Fancy Bear"),[26] that carried out the 2016 hack of the Democratic National Committee,[27] and Unit 74455 ("Sandworm"), that hacked power grids in Ukraine.[28] Even though less is known about its internal cyber structure,[29] the SVR has also carried out major operations, such as the SolarWinds hack in 2020.[30] Often these operations are launched from within Russia, but at other times, state hackers have gone abroad to attack targets. In 2018, for example, operatives from GRU Unit 26165 traveled to the Netherlands to hack into and disrupt the investigation of the Organization for the Prohibition of Chemical Weapons (OPCW) into the poisoning of Sergei Skripal and his daughter.[31] GRU Unit 26165 hackers, apparently part of the same sub-team of GRU Unit 26165, were also on site in Rio de Janeiro, Brazil and Lausanne, Switzerland to break into systems of the US Anti-Doping Agency, the World Anti-Doping Agency, and the Canadian Center for Ethics in Sport.[32]

Moscow finances and directs cyber and information operations through front organizations and websites used by the GRU, the SVR, and the FSB to spread disinformation.[33] The Russian government also uses companies like Neobit and AST to technically support cyber and information operations, with some companies acting like contractors but in a covert capacity.[34] It is possible that the Russian government is increasingly stationing these cyber and information assets overseas. One of the Russian spies the United States caught and deported in June 2010 was working at Microsoft. The man had no apparent links to the Russian intelligence community. However, federal authorities knew that he had previously worked at Neobit,[35] currently linked, per the US Department of the Treasury's April 2021 sanctions, to the Russian Ministry of Defense, the FSB, and the SVR.[36] In 2019, a Czech magazine reported that the Czech Security Information Service had shut down two private IT companies in early 2018 that were fronts for Russian hackers, reportedly part of a broader international network.[37] Outside of what the United States considers cyber operations, but well within the Russian government's cohesive conception of the information space, the Internet Research Agency has since 2016 been setting up overseas offices in Ghana, Nigeria, and Mexico to covertly run information operations.[38] Yevgeny Prigozhin, Putin's "chef" and confidante, heads these operations that, even while coordinated surreptitiously by the Kremlin, may not involve constant or direct government control.

The Russian government also recruits hackers and cybercriminals on an ad hoc basis to conduct operations.[39] Authorities allow the Russian cybercriminal apparatus to thrive for a variety of reasons, including the fact that cybercrime brings money into Russia, and the talent base it cultivates gives the Kremlin proxies to tap as needed. It is also part and parcel of the pervasive corruption in the Russian business and government world. Through the "social contract" these hackers have with the Kremlin, they generally get permission to operate freely, as long as they focus mainly on foreign targets and do not undermine the Kremlin's objectives. They must also be responsive to Russian government requests, even if the motives of these cybercriminals are primarily financial.[40] (In the rare, publicly reported instances of Russian authorities

25 US Library of Congress, Congressional Research Service, *Russian Cyber Units*, by Andrew S. Bowen, IF11718 (2022), 2, https://sgp.fas.org/crs/row/IF11718.pdf; "Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine," Palo Alto Networks, February 3, 2022 (updated June 22, 2022), https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/.

26 See, for example: "Investigative Report: On The Trail Of The 12 Indicted Russian Intelligence Officers," *RadioFreeEurope/RadioLiberty*, July 19, 2018, https://www.rferl.org/a/investigative-report-on-the-trail-of-the-12-indicted-russian-intelligence-officers/29376821.html.

27 US Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," July 13, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

28 See, for example: Andy Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *WIRED*, April 12, 2022, https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/; Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Penguin Random House, 2020).

29 Thanks to individuals who participated in a Chatham House Rule workshop on Russian cyber operations for discussion of this issue.

30 See, for example: US Cybersecurity & Infrastructure Security Agency (CISA), "Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders," April 26, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-116a.

31 "How the Dutch Foiled Russian 'Cyber-Attack' on OPCW," BBC, October 4, 2018, https://www.bbc.com/news/world-europe-45747472.

32 *United States of America vs. Aleksei Sergeyevich Morenets*, et al. (2018), 6, https://nsarchive.gwu.edu/document/17596-united-states-v-alexei-sergeyevich-morenets-et.

33 US Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections."

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

35 Benjamin Carlson, "Who Was the 12th Russian Spy at Microsoft?" *The Atlantic*, July 14, 2010, https://www.theatlantic.com/international/archive/2010/07/who-was-the-12th-russian-spy-at-microsoft/344876/; Sébastian Seibt, "Microsoft Entangled in Russian Spy Scandal," *France24*, July 15, 2010, https://www.france24.com/en/20100715-microsoft-entangled-russian-spy-scandal-alexey-karetnikov-swap.

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

37 "Czech Intel Reveals Russian Hackers Using IT Company Front: Media," UNIAN Information Agency, March 19, 2019, https://www.unian.info/world/10484166-czech-intel-reveals-russian-hackers-using-it-company-front-media.html.

38 Clarissa Ward et. al, "Russian Election Meddling Is Back – via Ghana and Nigeria – and in Your Feeds," CNN, April 11, 2020, https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html; US Office of the Director of National Intelligence, *Foreign Threats to the 2020 US Federal Elections*, March 2021, 4, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

39 To the reader, as part of the broader Kremlin recruitment of criminals, see: Mark Galeotti, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe* (Berlin: European Council on Foreign Relations, April 2017), https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/.

40 See, for example: Raymond Pompon recounting Russian cybercriminals complaining about the prospect of being coopted by the security services: Raymond Pompon, "Russian Hackers, Face to Face," F5, August 1, 2017, https://www.f5.com/labs/articles/threat-intelligence/russian-hackers-face-to-face.

arresting cybercriminals, the hackers involved had either stolen from or targeted Russian citizens.[41] Even former FSB-linked hackers may not be safe if they violate the Kremlin's social contract.[42]) As Nina Kollars and Michael Petersen write, "institutional boundaries have become porous, allowing private citizens and organizations to conduct sanctioned state activities and allowing the state to mine society for autonomous assets to carry out state functions."[43]

Several cases underscore how the Russian government recruits programmers and criminal hackers as needed, often through the FSB. In the late 2000s, the FSB reportedly contacted an individual tied to a patriotic hacker website in an attempt to establish a cooperative relationship.[44] Around the time of the Russo-Georgian War in 2008, Russian intelligence agencies tried to create an online forum to recruit hackers to attack Georgian targets.[45] In September 2015, the independent Russian news website Meduza reported that Alexander Vyarya, who worked at a Russian company building distributed denial-of-service (DDoS) defense software, said Rostec, Russia's defense conglomerate, approached him requesting his help to improve the government's DDoS attack capabilities.[46] Vyarya noted that, at a meeting in Sofia, Bulgaria, software developers showed him an existing Russian government DDoS capability, which was demonstrated on the websites of the Ukrainian Ministry of Defense and the Russian edition of *Slon.ru* (an online magazine);[47] Vyarya refused to get involved and then left Russia.[48] This last example illustrates an additional set of risks and incentives—those of individuals working as company programmers tapped by the Russian government to provide assistance who must assess the consequences of refusal.

In 2017, the US Department of Justice charged two FSB officers and their criminal collaborators with hacking into Yahoo and millions of email accounts.[49] The indictment alleged that the officers "conspired together and with each other to protect, direct, facilitate, and pay criminal hackers to collect information through computer intrusions in the US and elsewhere."[50] The document stated that the officers tasked hackers with targeting Yahoo email accounts; when they wanted information from non-Yahoo emails, they tasked a hacker and paid them a "bounty."[51] The indictment described one officer, in particular, as a hacker's "handling FSB officer."[52] Yet these FSB officers went a step beyond material direction and financing. In line with other nominally state-sanctioned criminal activities in Russia, the FSB officers allegedly provided one of the hackers with "sensitive FSB law enforcement and intelligence information that would have helped him avoid detection by law enforcement, including information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers."[53]

Other accounts describe parts of the Russian government, including the FSB, the GRU, and the Ministry of Internal Affairs, cultivating close relationships with nonstate hackers.[54] Positive Technologies, a Russian IT firm sanctioned by the US government, hosts conventions that the FSB and the

41 See, for example: "Russian hacker gang arrested over $25m theft," BBC, June 2, 2016, https://www.bbc.com/news/technology-36434104; Jeff Stone, "Rare Cybercrime Enforcement in Russia Yields 25 Arrests, Shutters 'BuyBest' Marketplace," *CyberScoop*, March 25, 2020, https://www.cyberscoop.com/buybest-hackers-arrested-fsb-russia/; Roman Zakharov, "Detentions in the Case of the Largest Group of Hackers Took Place in 11 Regions of the Russian Federation," Задержания по делу крупнейшей группировки хакеров прошли в 11 регионах РФ, *TV Zvevda*, March 24, 2020, https://tvzvezda.ru/news/2020324943-i7KCz.html.

42 "Russian Hackers Allegedly Tied to FSB and Hack of U.S. Democratic Party Handed Lengthy Prison Terms," *RadioFreeEurope/RadioLiberty*, February 14, 2022, https://www.rferl.org/a/russia-fsb-hackers-sentenced-democratic-party/31703350.html.

43 Nina A. Kollars and Michael B. Petersen, "Feed the Bears, Starve the Trolls: Demystifying Russia's Cybered Information Confrontation Strategy," *The Cyber Defense Review* (2019): 145–158, 148 https://cyberdefensereview.army.mil/Portals/6/Session%203%20Number%202%20CDR-Special%20Edition-2019.pdf.

44 "'It's Our Time to Serve the Motherland,'" Meduza, August 7, 2018, https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland; Andrei Soldatov, "Cyber Surprise," Кибер-сюрприз, *Novaya Gazeta*, May 30, 2007, https://novayagazeta.ru/articles/2007/05/31/33284-kiber-syurpriz.

45 Insikt Group, "Dark Covenant: Connections Between the Russian State and Criminal Actors," (Somerville: Recorded Future, September 2021), 4, https://www.recordedfuture.com/russian-state-connections-criminal-actors.

46 Daniel Turovsky, "Why Did the State Corporation Need a System for Organizing DDoS Attacks," Грузить по полной программе, Meduza, September 3, 2015, https://meduza.io/feature/2015/09/03/gruzit-po-polnoy-programme; Freid Weir, "In Russia's Cyberscene: Kremlin Desires, Private Hackers, and Patriotism," *The Christian Science Monitor*, October 27, 2016, https://www.csmonitor.com/World/Europe/2016/1027/In-Russia-s-cyberscene-Kremlin-desires-private-hackers-and-patriotism.

47 Turovsky, "Why Did the State"; Weir, "In Russia's Cyberscene."

48 Turovsky, "Why Did the State"; Weir, "In Russia's Cyberscene."

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

50 *United States of America v. Dmitry Dokuchaev, Igor Sushchin, Alexsey Belan, and Karim Baratov*, CR17-109 (2017), 2, https://www.justice.gov/opa/press-release/file/948201/download.

51 *United States of America v. D. Dokuchaev* et al., 3.

52 *United States of America v. D. Dokuchaev* et al., 3.

53 *United States of America v. D. Dokuchaev et al.*, 2–3.

54 See, for example: Insikt Group, "Dark Covenant"; Joe Cheravitch and Bilyana Lilly, "Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond," NATO Cooperative Cyber Defense Center of Excellence, December 2020, https://ccdcoe.org/uploads/2020/12/2-Russias-Cyber-Limitations-in-Personnel-Recruitment-and-Innovation_ebook.pdf, 31–59: 38–39; Flashpoint, "Russia Is Cracking Down on Cybercrime. Here Are the Law Enforcement Bodies Leading the Way," February 14, 2022, https://flashpoint.io/blog/russian-cybercrime-law-enforcement-bodies-fsb-mvd-deptk/; *United States of America vs. Yevgeniy Alexandrovich Nikulin*, CR 16-00440 WHA (2020), United States' Motion in Limine No. Six to Exclude Hearsay Statements by Nikita Kislitsin, 4, https://www.courthousenews.com/wp-content/uploads/2020/07/USANikulin-KislitsinMotion.pdf.

GRU use as recruiting events.[55] The US Treasury Department stated in April 2021 that the FSB cultivated and coopted the ransomware group Evil Corp.[56] The FSB had apparently given one of Evil Corp's alleged members, Igor Turashev, enough cover to register three Russian companies in his name, in a building known for crypto firm money laundering.[57] Despite this apparent brazenness, most nonstate hacker recruitment occurs in the more obscure corners of the Russian cyber web. As journalist and Russian intelligence expert Andrei Soldatov has said, "We know there is a huge pool of capable talent, and at least some people who are willing to do things that are suggested to them. We know such things are being done. What we don't know is how or why such orders are formulated, and who exactly may be involved."[58] To Soldatov's point, different elements of the Russian security apparatus may tap hackers for different purposes, ranging from strategic to highly tactical; nonstate hacker recruitment does not necessarily originate from the same level of the Russian government.

Beyond the outright backing and recruitment of nonstate cyber actors, the Kremlin also engages in other target activities, such as encouraging individuals to carry out cyber operations. Patriotic hacking groups are a prime example. These collectives, ranging from loosely to more formally organized, are composed of technically skilled people who conduct operations in line with government interests (or what they perceive as government interests). Some of these activities began with a domestic bent, such as the policing and targeting of regime critics online,[59] but have since expanded into the foreign arena. Following the Russia-originating cyber operations against Estonia in 2007, a representative of the Unified Russia party said his assistant—a member of the pro-Kremlin youth group Nashi—participated in the attacks.[60] During the 2008 Russo–Georgian War, it appears patriotic hackers may have taken part in launching DDoS attacks against Georgian websites.[61]

These individuals genuinely believe they are expressing patriotism for the Russian nation. An analysis of pro-Russian and pro-Ukrainian patriotic hacker Twitter posts between 2014 and 2017, after the Putin regime's invasion and annexation of Crimea, found that the hackers created a "popular, even populist identity" online based on patriotism.[62] In 2007, malicious web queries transmitted to Estonian websites by Russian actors (believed to be patriotic hackers) invoked false claims of fascism in reference to Andrus Ansip, Estonia's then-prime minister, with phrases such as "ANSIP_PIDOR=-FASCIST,"[63] echoing a nationalistic narrative espoused by members of the Russian parliament.[64]

Meduza reports that several Russian-speaking, nonstate hackers identified the 2008 Russo–Georgian War as a catalyst for Russian intelligence service recruitment of patriotic hackers.[65] There has recently been speculation about the Russian government encouraging the patriotic hacking of Ukrainian targets.[66] Yet, hacks of this kind are not always state-directed. Something as simple as a Kremlin official getting on TV and criticizing a foreign country might be the only prompt a patriotic hacker needs to act. After browsing online forums that shared software for possible use to attack Georgia, journalist Evgeny Morozov said in August 2008:

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

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

57 Joe Tidy, "Evil Corp: 'My hunt for the World's Most Wanted Hackers,'" BBC, November 17, 2021, https://www.bbc.com/news/technology-59297187; Kartikay Mehrotra and Olga Kharif, "Ransomware HQ: Moscow's Tallest Tower Is a Cybercriminal Cash Machine," *Bloomberg*, November 3, 2021, https://www.bloomberg.com/news/articles/2021-11-03/bitcoin-money-laundering-happening-in-moscow-s-vostok-tower-experts-say.

58 Weir, "In Russia's Cyberscene."

59 See, for example: Françoise Daucé, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva, "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia," *Russian Review of Social Research* 11, no. 3 (2019): 46–70; "Nashi Denies Cyberattack on Kommersant, Threatens Lawsuit," *Moscow Times*, February 9, 2012, https://www.themoscowtimes.com/2012/02/09/nashi-denies-cyberattack-on-kommersant-threatens-lawsuit-a12531. See also, on the Internet Research Agency: Adrian Chen, "The Agency," *New York Times Magazine*, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

60 Chloe Arnold, "Russian Group's Claims Reopen Debate On Estonian Cyberattacks," *RadioFreeEurope/RadioLiberty*, March 30, 2009, https://www.rferl.org/a/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html. On patriotic hacking, see also: Dorothy Denning, "Tracing the Sources of Today's Russian Cyberthreat," *Scientific American*, August 18, 2017, https://www.scientificamerican.com/article/tracing-the-sources-of-today-rsquo-s-russian-cyberthreat/.

61 Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008–2009), https://www.army.mil/article/19351/georgias_cyber_left_hook. See also, on the Russian Business Network criminal group some suspected was involved: Peter Warren, "Hunt for Russia's Web Criminals," *The Guardian*, November 15, 2007, https://www.theguardian.com/technology/2007/nov/15/news.crime.

62 Tetyana Lokot, "Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism," *Irish Studies in International Affairs* 28 (2017): 99–116, 113, https://www.jstor.org/stable/10.3318/isia.2017.28.9.

63 Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," NATO Cooperative Cyber Defense Center of Excellence, 2008, 2, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

64 Luke Harding, "Russia up in arms after Estonians remove statue of Soviet soldier," *The Guardian*, April 27, 2007, https://www.theguardian.com/world/2007/apr/28/russia.lukeharding.

65 Meduza, "It's Our Time to Serve the Motherland."

66 See, for example: Joe Tidy, "Russian Vigilante Hacker: 'I Want to Help Beat Ukraine from My Computer,'" BBC, February 25, 2022, https://www.bbc.com/news/technology-60528594.

> In less than an hour, I had become an internet solider. I didn't receive any calls from Kremlin operatives; nor did I have to buy a web server or modify my computer in any significant way.…Paranoid that the Kremlin's hand is everywhere, we risk underestimating the great patriotic rage of many ordinary Russians, who, having been fed too much government propaganda in the last few days, are convinced that they need to crash Georgian websites.[67]

Speculation also exists that the Russian government encourages patriotic hacking to provide cover for state-run operations.

Although these individuals and organizations have permission to operate independently, Moscow does not hide its affinity for these hackers or their cyber capabilities. In a June 2017 meeting with international media, Putin compared patriotic hackers to painters, saying that "hackers are free people. They are like artists. If they are in a good mood, they get up in the morning and begin painting their pictures."[68] He elaborated that "hackers are the same. They wake up in the morning, they read about some developments in international affairs, and if they have a patriotic mindset, then they try to make their own contribution the way they consider right into the fight against those who have bad things to say about Russia."[69] Explicitly directed or not, Putin is well aware that patriotic hackers are a component of the Russian cyber web that the government can leverage at will.

Otherwise, most Russian state involvement with nonstate hackers is ill-defined. The Russian hacking group Evil Corp, indicted by the United States in November 2019 and sanctioned that December, is an illustrative example.[70] The group is run by Maxim Yakubets, a Russian hacker reportedly married to Alyona Eduardovna Benderskaya, the daughter of Eduard Bendersky.[71] A former FSB Spetsnaz officer, Bendersky owns multiple private Russian security firms and, according to Bellingcat, is a "de-facto spokesman for Department V" or Vympel,[72] the FSB's externally focused "antiterrorist" unit that has carried out multiple overseas assassinations.[73] Since 2017, the year he and Bendersky's daughter presumably married, Yakubets.[74] Yakubets has been in the process of getting a Russian government security clearance since April 2018.[75] He is still at large in Russia, despite alleged Russian arrests of affiliates of a different ransomware group, REvil, in February 2022[76] that had provided a glimmer of (wishful) hope that Moscow was, in fact, actually cracking down on ransomware and other cybercriminal activity. One senior US official, for example, had—quite idealistically—told reporters following the REvil arrests that "these are very important steps, in that they represent the Kremlin taking action against criminals operating from within its borders, and they represent what we're looking for with regard to continued activities like these in the future."[77]

> "[Hackers] 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." —Vladimir Putin, June 2017

Putin does not control all these groups, and even if the FSB does engage with a hacker on a local level, Putin is (by and large) not involved in the day-to-day minutiae. Nevertheless, the Kremlin clearly allows cybercriminals and other nonstate hackers to thrive in Russia. Moreover, for the largest groups in the cyber web, the regime to a certain extent actively decides to look the other way. Given these circumstances, the next section discusses the benefits the regime gets, or perceives it gets, from leveraging this network of Russian cyber actors.

67 Evgeny Morozov, "An Army of Ones and Zeros," *Slate Magazine*, August 14, 2008, https://slate.com/technology/2008/08/how-i-became-a-soldier-in-the-georgia-russia-cyberwar.html.

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

69 Putin Compares Hackers To 'Artists,'" RadioFreeEurope/RadioLiberty.

70 *United States of America vs. Maskim V. Yakubets and Igor Turashev*, CR 19-342 (W.D. Pa., 2019), https://www.justice.gov/opa/press-release/file/1223586/download; US Department of the Treasury, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware," December 5, 2019, https://home.treasury.gov/news/press-releases/sm845.

71 "The FSB's Personal Hackers," Meduza, December 12, 2019, https://meduza.io/en/feature/2019/12/12/the-fsb-s-personal-hackers; Mark Krutov and Sergey Dobrynin, "Son in Law for 5 Million," Зять на 5 миллионов, *Svoboda*, December 9, 2019, https://www.svoboda.org/a/30315952.html.

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

73 US Library of Congress, *Russian Military Intelligence: Background and Issues for Congress*, by Andrew S. Bowen, R46616, Congressional Research Service, November 2021, 13 https://sgp.fas.org/crs/intel/R46616.pdf; "'V' for 'Vympel'"; "FSB's Magnificent Seven: New Links between Berlin and Istanbul Assassinations," *Bellingcat*, June 29, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/06/29/fsbs-magnificent-seven-new-links-between-berlin-and-istanbul-assassinations/.

74 US Department of the Treasury, "Treasury Sanctions Evil Corp."

75 Meduza, "The FSB's personal hackers"; US Department of the Treasury, "Treasury Sanctions Evil Corp."

76 Arielle Waldman, "Fallout from REvil arrests shakes up ransomware landscape," TechTarget, February 14, 2022, https://www.techtarget.com/searchsecurity/news/252513401/Fallout-from-REvil-arrests-shakes-up-ransomware-landscape.

77 James Rundle, Catherine Stupp, and Kim S. Nash, "What Russia's Arrest of REvil Hackers Means for Ransomware," *Wall Street Journal*, January 14, 2022, https://www.wsj.com/articles/what-the-russian-crackdown-on-revil-means-for-ransomware-11642188675.

THE RISKS AND BENEFITS OF THE CYBER WEB FOR THE KREMLIN

From the Kremlin's perspective, the web of Russian cyber actors—from nonstate patriotic hackers and cybercriminals to state-funded front companies—can provide numerous benefits. Principally, the returns include deniability, the power to wage covert political warfare below the threshold of outright war, and potentially reduced costs to maintain cyber capabilities. Additionally, the economic benefits should not be downplayed. While exact figures are hard to come by, cybercriminals are clearly bringing money into Russia, with billions of dollars estimated to have been raked in already by 2014.[78] In 2021 alone, it was reported that 74 percent of global ransomware revenue went to Russian hackers, to the tune of $400 million in cryptocurrencies.[79] That said, this activity also comes with many risks, including having to deal with competence and discipline issues that contribute to political-criminal tensions within hacking groups, undermining effectiveness. Recruiting from overlapping groups can also lead to political problems when the hackers act outside their remit or no longer work for the state but are identified as state actors. There is a simultaneous interplay between all these dynamics.

As noted, deniability is a pivotal factor in the Kremlin's strategic and operational decision-making. Putin is not a micromanager.[80] Instead, he operates an "adhocracy" that allows elites to "become policy entrepreneurs, seeking and seizing opportunities to develop and even implement ideas that they think will further the Kremlin's goals."[81] In practice, this creates ambiguity and, from the Kremlin's perspective, plausible deniability.[82] This approach is particularly conducive to cyber and information operations because they can be conducted remotely from behind a computer screen. Some argue that this deniability is implausible, correctly pointing out that Moscow often poorly obscures links between Kremlin officials and supposedly non-state-affiliated proxies,[83] such as in the case of the patriotic hackers targeting Estonia, Georgia, and Ukraine. In some instances, Russian officials blatantly lie, even when faced with overwhelming evidence to the contrary. In 2018, when Dutch intelligence caught and publicly exposed the GRU Unit 26165 operatives who flew to The Hague to disrupt the OPCW investigations, one retired Russian lieutenant general said, "You say this is evidence. It's not evidence to me. Russian intelligence was believed to be among the best in the world. Now you want to present a bunch of fools, absolutely incompetent, absolutely stupid, non-professional idiots? It's insulting."[84]

Regardless, the Kremlin does have periods when it can deny knowledge of, association with, and/or responsibility for cyber and information activities. While the ongoing war in Ukraine is an example of (Western) government intelligence exposing Russian plans and activities in near to real time, there are many prior instances when the state had plenty of time to deny cyber operations emanating from Russia before evidence emerged.[85] This ambiguity between the Russian government and cyber actors—whether a GRU front company or a ransomware group working with an FSB officer—gives the Kremlin space, however small, to claim no involvement. The fact that this is sometimes genuinely true, like when the Russian government permits cybercriminals to do what they want without actively supervising or directing them, helps bolster Moscow's objections. Moscow can engage with other governments knowing that sometimes, its denials of involvement are true and in cases when it is not (such as when the government is, at minimum, complicit in choosing not to investigate certain cyber operations), officials can lean into the ambiguity that surrounds its control over the Russian cyber web. Leveraging this extensive and opaque web of cyber actors also enables the Kremlin to make absurd demands of the United States, such as in June 2021, when Putin said that Russia would allow the extradition of cybercriminals to the United States, if the US government would agree to do the same for Russia.[86] Touting these bad faith gestures as genuine attempts at diplomacy is reminiscent of the Kremlin's legalistic approach to international norms

78 Tim Maurer, *Why the Russian Government Turns a Blind Eye to Cybercriminals*, *Carnegie Endowment for International Peace*, February 2, 2018, https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499.

79 Joe Tidy, "74% of Ransomware Revenue Goes to Russia-Linked Hackers," BBC, February 14, 2022, https://www.bbc.com/news/technology-60378009.

80 Fiona Hill and Clifford G. Gaddy, *What Makes Putin Tick, and What the West Should Do*, *Brookings Institution*, January 13, 2017, https://www.brookings.edu/research/what-makes-putin-tick-and-what-the-west-should-do/.

81 Mark Galeotti, "Russia Has No Grand Plans, but Lots of 'Adhocrats,'" *Intellinews*, January 18, 2017, https://www.intellinews.com/stolypin-russia-has-no-grand-plans-but-lots-of-adhocrats-114014/. See also: Mark Galeotti, "Russia's Murderous Adhocracy," *Moscow Times*, August 22, 2020, https://www.themoscowtimes.com/2020/08/22/russias-murderous-adhocracy-a71219. Thanks as well to Brian Whitmore for discussion of this point during the writing of my *Reassessing RuNet* report.

82 Lucian Kim, "In Putin's Russia, An 'Adhocracy' Marked By Ambiguity And Plausible Deniability," NPR, July 21, 2017, https://www.npr.org/sections/parallels/2017/07/21/538535186/in-putins-russia-an-adhocracy-marked-by-ambiguity-and-plausible-deniability.

83 See, for example: Paul Stronski, *Implausible Deniability: Russia's Private Military Companies*, *Carnegie Endowment for International Peace*, June 2, 2020, https://carnegieendowment.org/2020/06/02/implausible-deniability-russia-s-private-military-companies-pub-81954.

84 Sarah Rainsford, "Have Russian Spies Lost Their Touch?" BBC, October 6, 2018, https://www.bbc.com/news/world-europe-45762300.

85 To the reader, for instance, the Russian government has "vehemently denied accusations" of influence over cyber proxies active in the conflict in Ukraine. However, research by private sector cybersecurity companies has since suggested there are links between Russian cyber proxy groups and the Russian government. Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn: NATO Cooperative Cyber Defense Center of Excellence, 2015), 85, https://ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf. There are many other examples, for example: Jack Detsch, "How Russia and Others Use Cybercriminals as Proxies," *Christian Science Monitor*, June 28, 2017, https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies.

86 "Putin Says Russia Ready to Extradite Cyber Criminals to US on Reciprocal Basis," *TASS*, June 13, 2021, https://tass.com/russias-foreign-policy/1302315.

on cyber issues more broadly, with legal concepts about "sovereignty" cited to promote a government-controlled vision of the internet.[87] Furthermore, even if deniability is "implausible" to outside observers, that does not mean the claim is worthless. As Rory Cormac and Richard Aldrich have argued, implausible deniability can still exploit a target's decision-making gaps, building powerful narratives (e.g., around Putin's omnipotence) and signaling resolve, among other benefits.[88]

Leveraging the cyber web empowers Moscow to wage political warfare in what the West would call the "gray zone," below the threshold of armed conflict. The Russian state has a history of operating in the sphere of political warfare, and recent Russian military thinking has carried this mindset into the modern age. Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces and First Deputy Defense Minister, wrote an article in 2013 arguing that "the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[89] While often wrongly cited as the "Gerasimov doctrine," when it is neither a doctrine nor binding,[90] and often used to incorrectly argue that hybrid warfare is a new kind of Russian thinking,[91] the article nonetheless recognized the importance of nonmilitary tactics in modern conflict. As Eugene Rumer explains, Russia's foreign and military policy over the last two decades clearly emphasizes that "military power is the necessary enabler" of what many refer to as hybrid warfare, where "hybrid tools can be an instrument of risk management when hard power is too risky, costly, or impractical, but military power is always in the background."[92]

The Russian government can employ these measures continuously by leveraging the Russian cyber web both during war and peace. For decades, the Russian state has leveraged private Russian technology companies and their technical personnel to support state cyber and information operations. Through the FSB and other security agencies, the Kremlin has used hackers to assist with espionage and other activities below the threshold of armed conflict. It has even permitted ransomware and cybercriminal groups to thrive, so long as they toe the Kremlin's political line and focus on foreign targets. The Kremlin can also leverage cyber operators in gray zone conflicts, such as its illegal invasion and annexation of Crimea in 2014, and its encouragement of patriotic hackers to go after Ukrainian targets. From the Kremlin's perspective, all of this is an inherent benefit of having a large network of cyber actors to leverage as needed.

Operating in the gray zone with proxies also conveys the benefit of creating uncertainty for adversaries about how to respond. The cyber and information operations that targeted US elections, for instance, generated intense debates in the United States about if and how to respond; if a response were taken, concern about how to employ different ladders of escalation and to classify that action under international law resulted in the US government hesitating to take forceful action. According to the Senate Intelligence Committee's investigation into Russia's 2016 election interference, Obama administration officials were concerned about "appearing to act politically on behalf of one candidate, undermining public confidence in the election, and provoking additional Russian actions."[93] This reluctance to act, including the associated political concerns, illustrates the benefit the Russian government receives from the below-threshold nature of internet-based political warfare. Individual actors might engage in phishing and ransomware attacks most days of the week, with one day set aside to steal data for a GRU officer. In this way, Moscow effectively blurs the lines between criminal activity, independent technology development, and espionage, muddling Western policy responses.

Finally, the ability to tap into a nebulous web of cyber actors also means that the Kremlin can leverage capabilities without the need to constantly supervise everything. There is, once again, a spectrum of financial, training, and supervisory costs. The front companies that run FSB, SVR, and GRU cyber and information operations ostensibly pay for those activities themselves, leveraging intelligence personnel (although that is unclear). The Internet Research Agency and state-supporting companies like Neobit operate in an undefined zone,

87 Dennis Broeders, Liisi Adamson, and Rogier Creemers, *Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace*, Social Science Research Network, December 2019, 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3493600.

88 Rory Cormac and Richard J. Aldrich, "Grey is the New Black: Covert Action and Implausible Deniability," *International Affairs* 94, no. 3 (May 2018): 477–494, 487, 490–491.

89 Valery Gerasimov, "The Value of Science in Foresight," Ценность науки в предвидении, *VPK-News*, February 26, 2013, https://vpk-news.ru/articles/14632; Valery Gerasimov, "The Value of Science Is in the Foresight," *Military–Industrial Courier*, February 27, 2013, translated June 2014 by Robert Coalson, published in *Military Review* (January–February 2016), 24, https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.

90 See, for example: Nicole Ng and Eugene Rumer, *The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture*, *Carnegie Endowment for International Peace*, July 3, 2019, https://carnegieendowment.org/2019/07/03/west-fears-russia-s-hybrid-warfare.-they-re-missing-bigger-picture-pub-79412; Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

91 To the reader, for a good treatment of this issue and the terminology "hybrid warfare," see: Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (London: Routledge, December 2020).

92 Eugene Rumer, *The Primakov (Not Gerasimov) Doctrine in Action*, *Carnegie Endowment for International Peace*, June 2019, 1, https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.

93 US Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 US Election. Volume 3: U.S. Government Response to Russian Activities*, 116th Congress, 116–XX, February 2020, 3, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf.

where Putin cronies spend state-granted wealth and the Russian government contracts nonstate support and capabilities. Then there are the many cybercriminals, patriotic hackers, legitimate Russian IT company employees, and others who may operate independently, but do so with the state's permission and may receive requests to redirect resources to government activities. The publicly available evidence is anecdotal, but these efforts sometimes cost the government next to nothing. In the previously mentioned 2017 indictment of two FSB officers, one of the hackers confessed that he was paid about $100 "for each successful hack," wired by the FSB through PayPal, WebMoney, and other non-Russian online payment systems.[94]

While leveraging non-state actors in the Russian cyber web saves the Kremlin resources in some cases, the government may have to deal with competence and discipline issues;[95] cybercriminals might not operate with the same diligence as state hackers. Individual programmers recruited to develop capabilities for the state are likely untrained in Russian government methods of secrecy protection. Patriotic hackers might not use very sophisticated tools and instead, as the reporting suggests, use off-the-shelf capabilities posted on web forums.

Dueling political and criminal dynamics can also generate internal fractions within hacker groups, which affects their ability to operate for the state. Leaked documents from the Russian hacker group Conti, for instance, highlighted divisions over the group's official position on the war in Ukraine.[96] The government itself might not coordinate operations very well either. Analysts already debate whether or not the GRU and the FSB coordinated the hacks on the Democratic National Committee in 2016,[97] and the Russian security services, in general, have a long history of turf wars and infighting.[98] It is possible that multiple Russian security organizations—or even multiple units within a single Russian security organization—recruit hackers for overlapping purposes, such as developing information interception capabilities or launching destructive cyber operations that generate additional complexities.

There is also the risk of an actor becoming so closely associated with the government that they create problems when they act in line with their own preferences—the actor or group may no longer be working with the Russian government, but others might assume otherwise. Theoretically, a Russian government agent could be held internally responsible for this kind of activity, with superiors believing that the agent was sanctioning a cybercriminal operation like stealing from Russians or going after politically sensitive targets abroad. Other hypothetical cases could involve an entire government organization being blamed by the Kremlin for how it handled a relationship with a cyber web actor. In this sense, the risk of cyber actors behaving out of line could range from individual-level repercussions to broader ones, generating a different set of issues for government officers to worry about. Some scholars have argued that, in general, governments empowering proxies with "more expansive, or less restrained, political agendas" can lead to escalatory situations,[99] although that remains unclear in practice.

94 *United States of America v. Karim Baratov*, No. 17-CR-103 VC (2017), Plea Agreement, 5, https://www.justice.gov/usao-ndca/page/file/1021221/download. See more at: https://www.justice.gov/usao-ndca/us-v-dmitry-dokuchaev-et-al.

95 Galeotti, *Russian Political War*, 83. To the reader, "deniability and the opportunity to pick up 'off the shelf' assets often come at the expense of competence and discipline."

96 Christopher Whyte, "Leaked Hacker Logs Show Weaknesses of Russia's Cyber Proxy Ecosystem," *CSO Online*, March 29, 2022, https://www.csoonline.com/article/3655075/leaked-hacker-logs-show-weaknesses-of-russia-s-cyber-proxy-ecosystem.html.

97 See, for example, Robert Morgus, "Whodunnit? Russia and Coercion Through Cyberspace," War on the Rocks, October 19, 2016, https://warontherocks.com/2016/10/whodunnit-russia-and-coercion-through-cyberspace/; "It's a Feature, Not a Bug: Discord Observed in Russian Intelligence Operations," Horkos, September 20, 2018, https://horkos.medium.com/its-a-feature-not-a-bug-discord-observed-in-russian-intelligence-operations-2e2e79c4c8cc; "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/.

98 Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence* (New York: MacMillan, 2015). See also, in the cyber context specifically: Kimberly Zenz, "Infighting Among Russian Security Services in the Cyber Sphere," Black Hat USA, 2019, https://i.blackhat.com/USA-19/Thursday/us-19-Zenz-Infighting-Among-Russian-Security-Services-in-the-Cyber-Sphere.pdf.

99 Borghard and Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?"

RECOMMENDATIONS AND CONCLUSION

Putin does not control every cyber operation within Russia, nor does the Russian government manage every single cyber actor in the country. It is highly unlikely that senior Kremlin officials are discussing a small-scale Russian phishing ring or a group of Russian hackers targeting Western credit card companies. FSB officers who recruit cybercriminals on an as-needed basis likely have no desire to manage the day-to-day activity of that cybercriminal operation. However, the Putin regime inherited, and now cultivates, an extensive network of cyber actors in Russia. The government rarely engages with some elements of this network, even at a local law enforcement level, but it recruits, encourages, and may even directly finance other constituencies. Moscow creates an environment in which cybercrime thrives (including by permitting corruption to flourish) and, in doing so, protects many cybercriminals in Russia. The United States and its allies and partners must gain a better understanding of this network and of Russian cyber and information capabilities, especially as they try to disrupt operations coming out of Russia. Russia should also act as a case study for how a government can cultivate and leverage a large web of cyber and information actors to augment its power. In particular, the United States and its allies and partners should note and consider the following actions.

- **Takeaway:** The Putin regime perceives that it benefits—and in many cases, does materially benefit—from leveraging the Russian cyber web because it can claim deniability, has more power to wage covert political warfare below the threshold of outright war, and has potentially lower costs for cyber capabilities. Cybercriminals also bring money into Russia, an increasingly important factor for a heavily sanctioned country with a declining economy. Overall, the Putin regime has many incentives for continuing to allow cybercrime to thrive in Russia, as well as for creating front companies, leveraging cybercriminals and patriotic hackers, filching private company employees, and letting PMCs develop cyber capabilities.

- **Action:** US policymakers, working with allies and partners, should focus more on understanding the incentive structure behind the Russian cyber web, the wide range of actors within it, and the relationships those actors have with the Russian government at different points in time. Some US public messaging—such as policymaker excitement about Moscow's reported "arrests" of REvil ransomware members—does not reflect (or perhaps does not demonstrate) an understanding of the Russian government's incentives vis-à-vis these groups. Alongside conversations about how to disrupt particular activities, US policymakers should also focus on understanding these particular incentives. For example, cybercriminals who target individuals in Russia as well as the United States are much more likely to attract Russian government enforcement actions than cybercriminals who just target US individuals. This would be a relatively more effective area to direct US law enforcement cooperation with Russia than, say, ransomware actors who have no impact on the Russian population. Targeting cybercriminals who moonlight as government hackers to "put them out of business" could similarly leverage the incentive structure of the Russian cyber web by indirectly going after the state's capabilities. If these cybercriminals cannot afford to keep the lights on, then those hackers are *also* unable (at least in the immediate sense) to use those capabilities for the state's benefit when the government comes knocking. US policymakers must understand this incentive structure to develop the most effective responses.

- **Takeaway:** Putin does not control every cyber operation conducted within and from Russia. Although he personally ordered the efforts to influence the 2016 US election,[100] many cybercriminals (like those conducting phishing scams) do not receive direct instructions from the top levels of the Russian government. There are also many elements of Russia's security apparatus that recruit nonstate hackers directly (e.g., through a local FSB office), which means that high-level Kremlin knowledge of specific recruitment activities is unclear. Nonetheless, the fact remains that the Putin regime cultivates and actively leverages different actors in the Russian cyber web, and it could take action against specific groups if it chooses.

- **Action:** The US government should be precise about how it specifies and communicates the type of relationship the Russian government has with a given Russian cyber actor. If US policymakers continue to engage with the Putin regime about cracking down on nonstate hackers, particularly cybercriminals, they should identify whether the state actively recruited or engaged with a particular hacking entity before branding it a state-affiliated actor. Within the realm of state-linked actors, the US government should specify in public messaging, internally or in private discussions with Russian counterparts—depending on the case—what that link looks like, such as financing and supervision, ad hoc recruitment, or tacit approval. This matters because establishing any consistency or escalation ladder in the US response will require matching that response to factors such as the group, the group's actions, and the degree of Russian government involvement. The need for consistency also applies to public messaging, accurately distinguishing between espionage, disruptive attacks, hack-and-leak operations, and other actions. The degree of Russian government involvement in a cyber operation or with a cyber group may determine whether the responses taken by the United States and its allies and its partners target the actor behind the keyboard or specific parts of the Russian government. This is not to say that the Putin regime does not share responsibility for allowing a cybercriminal ecosystem to flourish (it does), nor

100 US Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, ICA 2017-01D, January 2017, ii, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

that the prospects for US–Russian diplomatic engagement on cyber operations are great (they are not),[101] but that an effective response must begin with a nuanced grounding in the Kremlin's spectrum of engagement with hackers.

- **Takeaway:** Even though modern internet capabilities enable unprecedented levels of microtargeting and global reach, Russian government thinking around information technology draws on decades of Russian political and security culture. Russian thinking centers around information security, taking a sweeping view of the modern information environment and how the state should shape it. This view does not make the same, firm distinctions between cyber operations (e.g., in code) and information operations (e.g., in human-readable content) that the United States and its allies and partners do. Cyber and information operations reside within a broad set of Russian government political warfare activities, which, on the whole, emphasize deniability, covertness, the use of proxies, and operations below the threshold of armed conflict, among others.

- **Action:** When talking, writing, and thinking about Russian cyber and information operations, US, ally, and partner policymakers, as well as intelligence analysts, must focus on the Russian government's unique views on the internet and information space, rather than projecting their own perspectives. Unfortunately, too many publications and analyses from the United States and other governments fail to grasp Russia's viewpoints, such as dismissing Russian statements about the global internet as mere propaganda and not genuine Kremlin belief. This is not to say that the Kremlin's more paranoid views about color revolutions or the internet as a CIA project are legitimate, nor that Moscow's thinking is the most effective in practice. Perhaps the concept of information security is beneficial for its perceived cohesion, or, possibly, because it becomes so encompassing that it hampers actual operational and tactical action. However, understanding the Kremlin's view of cyber and information activity, and situating it within other Russian thinking about political warfare and nonmilitary means of conflict, will move the United States and its allies and partners toward a more accurate picture of Russian cyber and information behavior. Arriving at this deeper understanding of Kremlin thinking will help the United States calibrate better policy responses to Russian government behavior, as well as predict how Moscow might respond to certain US actions.

It is impossible to predict how the Russian cyber ecosystem will evolve in the coming months and years, particularly as Western sanctions continue to erode the Russian economy. Additionally, Russia is facing an IT "brain drain," with technological talent fleeing the country for more economically stable—as well as freer and safer—work environments. That said, Russia's web of cyber actors does not appear to be disappearing, which makes deciphering it all the more vital for grappling with the Kremlin's political warfare and how it uses nonstate actors to augment cyber and information power.

101 See, for example: Andrei Soldatov, "Can the U.S. Still Cooperate with Russia's Security Agencies?" *Moscow Times*, May 14, 2021, https://www.themoscowtimes.com/2021/05/14/can-the-us-still-cooperate-with-russias-security-agencies-a73900.

ACKNOWLEDGMENTS

The author would like to thank Gavin Wilde, John Sipher, Cara Dienst, Dylan Myles-Primakoff, Sean Atkins, and an additional individual who shall remain anonymous for their feedback on an earlier version of this document. The author would also like to thank the individuals who participated in a Chatham House Rule discussion about this issue brief.

AUTHOR BIO

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, where his work focuses on the geopolitics, governance, and security of the global internet. He is also a senior fellow at Duke University's Sanford School of Public Policy and a contributor at WIRED Magazine.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
*Rafic A. Bizri
*Linden P. Blue
Adam Boehler
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
Beth Connaughty
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
Mark T. Esper
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Amir A. Handjani
Frank Haun
Michael V. Hayden
Amos Hochstein
Tim Holt
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Ashraf Qazi
Robert Rangel
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of July 13, 2021