Atlantic Council
EURASIA CENTER

CYBER STATECRAFT
INITIATIVE

RUSSIA TOMORROW:
NAVIGATING A NEW PARADIGM

CONFRONTING RUSSIA'S CYBER POWER:

Reassessing assumptions, sizing up the threat, and building a proactive response

Justin Sherman

Atlantic Council
EURASIA CENTER

CYBER STATECRAFT INITIATIVE

RUSSIA TOMORROW:
NAVIGATING A NEW PARADIGM

Russia's full-scale invasion of Ukraine in February 2022 challenged much of the common Western understanding of Russia. How can the world better understand Russia? What are the steps forward for Western policy? The Eurasia Center's new "Russia Tomorrow" series seeks to reevaluate conceptions of Russia today and better prepare for its future tomorrow.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

ISBN: 978-1-61977-375-2

May 2025

Design: Donald Partyka and Amelie Chushko

Cover: Illustration, Wikimedia

Atlantic Council
EURASIA CENTER

CYBER STATECRAFT
INITIATIVE

RUSSIA TOMORROW:
NAVIGATING A NEW PARADIGM

CONFRONTING RUSSIA'S CYBER POWER:

Reassessing assumptions, sizing up the threat, and building a proactive response

Justin Sherman

TABLE OF CONTENTS

INITIAL EXPECTATIONS

When the Russian government launched its full-scale invasion of Ukraine on February 24, 2022, many Western observers braced for digital impact—expecting Russian military and security forces to unleash all-out cyberattacks on Ukraine. Weeks before Moscow's full-scale war began, *Politico* wrote that the "Russian invasion of Ukraine could redefine cyber warfare." The US Cybersecurity and Infrastructure Security Agency (CISA) worried that past Russian malware deployments, such as NotPetya and WannaCry, could find themselves mirrored in new wartime operations—where the impacts would spill quickly and globally across companies and infrastructure. Many other headlines and stories asked questions about how, exactly, Russia would use cyber operations in modern warfare to wreak havoc on Ukraine. Some of these questions were fair, others clearly leaned into the hype, and all were circulated online, in the press, and in the DC policy bubble ahead of that fateful February 24 invasion.

As the Putin regime's illegal war unfolded, however, it quickly belied these hypotheses and collapsed many Western assumptions about Russia's cyber power. Russia didn't deliver the expected cyber "kill strike" (instantly plummeting Ukraine into darkness). Ukrainian and NATO defenses (insofar as NATO has spent considerable time and energy to support Ukraine on cyber defense over the years) were sufficient to (mainly) withstand the most disruptive Russian cyber operations, compared at least to pre-February 2022 expectations. And Moscow showed serious incompetencies in coordinating cyber activities with battlefield kinetic operations. Flurries of operational activity, nonetheless, continue to this day from all parties involved in the war—as Russia remains a persistent and serious cyber threat to the United States, Ukraine, and the West. Russia's continued cyber activity and major gaps between wartime cyber expectations and reality demand a Western rethink of years-old assumptions about Russia and cyber power—and of outdated ways of confronting the threats ahead.

Russia is still very much a cyber threat. Patriotic hackers and state security agencies, cybercriminals and private military companies, and so on blend together with deliberate state decisions, Kremlin permissiveness, entrepreneurialism, competition, petty corruption, and incompetence to create the Russian cyber web that exists today. The multidirectional, murky, and dynamic nature of Russia's cyber ecosystem—relying on a range of actors, with different incentives, with shifting relationships with the state and one another—is part of the reason that the Russian cyber threat is so complex.

Policymakers in the United States as well as allied and partner countries should take at least five steps to size up and confront Russia's cyber threat in the years to come:

- When assessing the expectations-versus-reality of Russia's wartime cyber operations, distinguish between capabilities and wartime execution.
- Widen the circle of analysis to include not just Russian state hackers but the broader Russian cyber web, including patriotic hackers and state-coerced criminals.
- Avoid the trap of assuming Russia can separate out cyber and information issues from other bilateral, multilateral, and security-related topics—maintaining its hostility toward Ukraine while, say, softening up on cyber operations against the United States.
- Continue cyber information sharing about Russia with allies and partners around the world.
- Invest in cyber defense and in cyber offense where appropriate.

RUSSIA'S CYBER ECOSYSTEM

Russia is home to a complex ecosystem of cyber actors. These include military forces, security agencies, state-recruited cybercriminals, state-coerced technology developers, state-encouraged patriotic hackers, self-identified patriotic hackers acting of their own volition, and more. Even Russian private military companies offer cyber operations, signals intelligence (SIGINT), and other digital capabilities to their clients. Together, these actors form a large, complex, often opaque, and dynamic ecosystem. The Kremlin has substantial power over this ecosystem, both guiding its overall shape (such as permitting large amounts of cybercrime to be perpetuated from within Russia) and leveraging particular actors as needed (discussed more below). Simultaneously, decisions aren't always top-down, as entrepreneurial cybercriminals and hackers—much like "violent entrepreneurs" in Russian business and crime, or the "adhocrats" vying for Putin's ear to pitch ideas—take initiative, build their own capabilities, and sell them to the state as well.

The relationships that different security agencies, at different levels, in different parts of the country and world, have with Russian hackers also vary over time. A local security service office might provide legal cover to a group of criminal hackers one day (after the necessary payoffs change hands, of course), only for a Moscow-based team to recruit them for a state operation the next. While the Kremlin has a sort of "social contract" with hackers—focus mainly on foreign targets; don't undermine the Kremlin's geopolitical objectives; be responsive to Russian government requests—its tolerance for a specific cybercriminal group can change on a whim, too. Security officials might take a bribe from a cybercriminal, much as their colleagues do on the regular, and still find their patrons in prison and their own wrists in handcuffs.

On the Russian government side, the principal units involved in offensive cyber operations are the Federal Security Service (FSB), the military intelligence agency (GRU), and the Foreign Intelligence Service (SVR). Russia does not have a proper, centrally coordinating cyber command; it was never launched despite attempts in the 2010s. The Ministry of Defense's initial efforts to make one happen by circa 2014 were, it came to be understood later, overtaken by the subsequent establishment of Information Operations Troops with seemingly some coordinating functions—though experts still debate its analogousness to a "cyber command" and its level of shot-calling compared to bodies like the Presidential Administration. So while it is possible for the Russian security agencies to coordinate their (cyber) operations with one another, their engagements are marked more by competition than cooperation.

Primary Russian government cyber actors

Federal Security Service (FSB)	Main Intelligence Directorate (GRU)	Foreign Intelligence Service (SVR)
Major FSB cyber units include the FSB's Center 16, focused on signals intelligence (SIGINT), and its Center 18, involved in domestic cyber operations and some foreign ones. The FSB touches a range of cyber activity from hack-and-leaks abroad to the targeting of dissidents to liaising with ransomware groups.	Major GRU cyber units include GRU Unit 26165 ("Fancy Bear"), which also engages in on-site hacking operations, Unit 74455 ("Sandworm"), which has been tied to many destructive attacks, and Unit 54777, which carries out psychological and information operations. Culturally, the GRU's cyber operations align with its kinetic operations–often more brazen, destructive, and disruptive.	Less is known publicly about the SVR's internal cyber structure compared to that of the FSB and GRU, although it has been associated with the state-involved hacker group known as "Cozy Bear." Culturally, the SVR's cyber operations align with its human operations–focused on quiet espionage and information-exfiltration rather than louder sabotage, as evidenced by its SolarWinds cyber intelligence operation.

Source: Author

The most prominent example of this potential overlap or inefficiency is when GRU-linked APT28 and SVR-linked APT29 both hacked the Democratic National Committee in 2016, making it unclear whether each knew the other was carrying out a similar campaign. This operational friction is exacerbated by the fact that the agencies' general remits—SVR on human intelligence, for instance, and FSB mostly domestic—do not translate to the digital and online world. All three agencies hack military and civilian targets and, for example, the FSB actively targets and hacks organizations outside of Russia's borders. Each agency approaches cyber operations differently, too, often in line with their overall institutional cultures—such as the GRU, known for its brazen kinetic operations including sabotage and assassination, carrying out the boldest and most destructive cyber operations, contrasted with the SVR, and its emphasis on secrecy, focusing on quiet cyber intelligence gathering like in the SolarWinds campaign. Still, the Russian state agencies with cyber operations remain active threats to the United States, Ukraine, the West, and plenty of others through intelligence-gathering efforts, disruptive operations, and efforts that meld both, such as hack-and-leak campaigns.

Beyond government units themselves, the state encourages patriotic hackers—sometimes just young, technically proficient Russians—to go after foreign targets through televised and online statements (such as disinformation about Ukraine). Different security organizations, such as the FSB, may hire

cybercriminals for specific intelligence operations and pay them based on the targets they penetrate. Other private-sector companies pitch their own services to the state of their own volition, bid on government contracts, and support a range of offensive capability development, research and development, and talent cultivation efforts (including defensive activities and benign or even globally cybersecurity-positive activities beyond the scope of this paper). Russian private military companies increasingly offer capabilities related to SIGINT to their private and government clients around the world, too. All the while, the state retains the capability to target specific people and companies in Russia that otherwise have nothing to do with the state, apply the relevant pressure, and compel them to assist with state cyber objectives, which it can wield to extraordinary effect.

As the historian Stephen Kotkin notes, "The Russian state can confound analysts who truck in binaries." While there are several core themes to this ecosystem—complexity; state corruption; overwhelming tolerance for and even tacit support of cybercrime; myriad offensive cyber actors in play—Russia's cyber ecosystem neither fits into a neat box nor is a neatly run one at that.

For all the threats these actors pose to Ukraine and the West, assuming that the Putin regime controls all cyber activity emanating from within Russia's borders is not just inaccurate (e.g., the country's too big; there are too many players; it's not all top down), but is the kind of assumption that serves as a "useful fiction" for the Kremlin. It makes the system appear ruthlessly efficient and coordinated, gives disconnected or tactically myopic actions a veneer of larger strategy, and puts Putin at the center of all cyber operation decision-making. Thinking as much can, intentionally or not, further feed into the idea that the Kremlin's motives are clear and fixed or driven by some kind of "hybrid war" strategy. It also obscures the fact that—unlike many Western countries that do, in fact, publish official "cyber strategies"—Russia does not have a defined cyber strategy document, instead drawing on a range of documents and sweeping "information security" concepts to frame information, the internet, and cyber power.

On the contrary, it is the multidirectional, murky, and dynamic nature of Russia's cyber ecosystem that makes cyber activity subject to sudden change, feeds opportunities for interagency rivalries, contributes to effects-corroding corruption and competition, and provides the Kremlin with a spectrum of talent, capabilities, and resources to tap, direct, and deny (plausibly or implausibly) as it needs. It is in part this dynamism and multidirectional nature that makes Russia's cyber threat so complex—as mixes of deliberate state decisions, Kremlin permissiveness, entrepreneurialism, competition, petty corruption, and incompetence blend together to create the Russian cyber web that exists today. Relationships between the state proper, at different levels, in different organizations, with nonstate cyber affiliates are often shifting; ransomware groups persistently targeting Western critical infrastructure, for example, may be prolific for months before collapsing under internal conflict and reconstituting into new groups, with new combinations of the old tactics and talent. It is also the reason that what is known to date about cyber operations during Russia's full-out war on Ukraine provides such a valuable case study in assessing the status quo of this ecosystem—and, coupled with lessons from past incidents (like Russian cyberattacks on Estonia in 2007, Georgia in 2008, and Ukraine in 2014), helps to better weigh the future threat.

WHAT HAPPENED TO RUSSIA'S CYBER MIGHT?

Cyber operations have played a substantial role in Russia's full-on invasion of Ukraine in February 2022 and the ensuing war. These activities range from distributed denial of service (DDoS) attacks knocking Ukrainian websites offline and Ukrainian patriotic hackers' attacks on Russian government sites (what Kyiv calls its "IT Army") to Russia using countless malware variants to exfiltrate data and targeting Ukrainian Telegram chats and Android mobile devices. Without getting into a timeline of every major operation—neither this paper's focus nor possible given limits on public information—it is clear that Russian and Ukrainian forces and their allies, partners, and proxies have made cyber operations part of the war's military, intelligence, and information dimensions.

There are many ways to define cyber power, which is by no means limited to offensive capabilities. In Russia's case, analysts could focus on anything from Russia's national cyber threat defense system—the Monitoring and Administration Center for General Use Information Networks (GosSOPKA), which effectively brings together intrusion detection, vulnerability management, and other technologies for entities handling sensitive information—to the enormous IT brain drain problems the country suffered immediately following the full-on invasion of Ukraine. As explored in a study last year for the Atlantic Council, Russia's growing digital tech isolationism—both a long-standing goal and increasing reality for the Kremlin—has driven more independence in some areas, like software, while heightening dependence and strategic vulnerability in others, such as dependence on Chinese hardware. This paper's focus, though, will remain on Russia's offensive capabilities.

Pre-February 2022 expectations in the United States and the West, as highlighted above, were dominated by those predicting extensive Russian disruptive and destructive cyber operations. In these scenarios, Russia would leverage its state, state-affiliated, state-encouraged, and other capabilities to cause serious damage to Ukrainian critical infrastructure (telecommunications, water systems, energy grids, and so forth) and cleanly augment its kinetic onslaught. Russia would "employ massive cyber and electronic warfare tools" to collapse Ukraine's will to fight through digital means.

To be sure, some predictions were more measured. Some pointed to the 2008 Russo-Georgian War, as an illustration of Russian forces effectively using DDoS attacks (Moscow's shatter-communications approach) in concert with disinformation and kinetic action to prepare the battlefield, and conjectured that Moscow would do the same if it moved troops further into Ukraine. Others

highlighted Russia turning off Ukrainian power grids as a possible menu option for Moscow as it escalated. Cybersecurity scholars Lennart Maschmeyer and Nadiya Kostyuk, contrary to widely held positions, argued two weeks before Russia's full-scale invasion that "cyber operations will remain of secondary importance and at best provide marginal gains to Russia," incisively noting that press headlines talking of "cyber war" rest on "the implicit assumption that with the change in strategic context, the role of cyber operations will change as well." The overwhelming sentiment, though, was worry and anticipation of what some considered true, cyber-enabled, twenty-first century warfare.

But the cyber operations that unfolded immediately before and after the February 2022 invasion defied what many Western (including American) commentators were predicting. Russia didn't deliver the cyber kill strike expected (instantly plummeting Ukraine into darkness). Ukrainian and NATO defenses were sufficient to (mainly) withstand the most disruptive FSB and GRU cyber operations, compared at least to pre-February 2022 expectations. And Moscow showed serious incompetencies in coordinating cyber activities with battlefield kinetic operations. Many experts who did not expect cyber-Armageddon per se have still been surprised by the limited impact of Russian attacks, the focus on wiper attacks (that delete a system's data via malware) and data gathering over critical infrastructure disruptions, and apparent poor coordination between cyber and kinetic moves made by the Russian Armed Forces and intelligence services.

What, then, explains the gulf between expectations—decisive moves, cleanly executed operations, and visible results—and reality, with some operations, certainly, but the overwhelming focus on kinetic activity and far less on destructive cyber movement than anticipated? Scholars and analysts have, since February 2022, put forward several buckets of hypotheses.

Various commentators argue, as National Defense University scholar Jackie Kerr compiles and breaks down, that Russia's weak integration of cyber into offensive campaigns was symptomatic of broader problems with Russian military preparations for full-on war; that Western observers simply overestimated Russia's cyber capabilities; that poor coordination and competition between Russian security agencies impeded operational success; or that Ukraine's cyber defenses have been extraordinarily robust. Some have gone so far as to attribute Ukrainian cyber defenses, backed up by Western allies and partners, as the primary reason for Russian offensive failures. Russia cyber and information expert Gavin Wilde argues that Russia focused on countervalue operations (against civilian infrastructure, to demoralize political leaders and the public) more than counterforce operations (against Ukrainian military capabilities), to little effect, "a sign of highly sophisticated intelligence tradecraft being squandered in service of a deeply flawed military strategy."

Professors Nadiya Kostyuk and Erik Gartzke write that Russia's full-on war on Ukraine is about territory and physical control, making physical military activity far more important than cyber operations themselves. Cyber scholar Jon Bateman argues that traditional signals jamming and Russia's cyberattack against the Viasat satellite communications system, coupled with a chaotic slew of data-deletion attacks, may have helped Russia initially—but that cyber operations from there had diminishing novelty and impact. Russia's poor strategy, insufficient intelligence preparation, and interagency mistrust have been presented as causes for undermining Russia's cyber-kinetic strike coordination,

Selected February and March 2022 Russian cyber operations against Ukraine

- **February 15:** DDoS attacks on websites of Ukrainian Defense Ministry and Ukranian banks Privatbank and Oschadbank,[a] later attributed to the GRU.[b]
- **February 23:** "HermeticWiper" wiper malware used against Ukrainian government contractors in Latvia and Lithuania—and a Ukrainian financial institution.[c]
- **February 24:** "IsaacWiper" wiper malware deployed against another Ukrainian government network.[d]
- **February 24:** Cyberattack disrupted Ukrainian access to modems that deliver broadband satellite internet access from the company Viasat.[e]
- **February 25:** Hackers released updated "IsaacWiper" version.[f]
- **March 2:** DDoS attack on website of Ukrainian Ministry of Defense launched via malware-as-a-service platform (which sells subscriptions to hacking tools).[g]
- **March 2:** Russian activity detected within a Ukrainian nuclear power-plant network, the day before the Russian forces physically attacked and overtook it[h] (ostensibly, the Zaporizhzhia plant).[i]
- **March 15:** New "CaddyWiper" wiper malware strain used against Ukrainian organizations.[j]
- **March 18:** Ukraine warned of phishing campaign to exfiltrate data from Ukrainian targets.[k]

Sources: In addition to the sources cited below, the author thanks Kyle Fendorf and Jessie Miller at the Council on Foreign Relations for their compilation of incidents in March 2022, many of which are cited and briefly detailed in this graphic.

---

a Jenna McLaughlin, "Ukraine Says Government Websites and Banks Were Hit with Denial of Service Attack," NPR, February 15, 2022, https://www.npr.org/2022/02/15/1080876311/ukraine-hack-denial-of-service-attack-defense.

b United Kingdom government, "UK Assesses Russian Involvement in Cyber Attacks on Ukraine," February 18, 2022, https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine.

c Dan Milmo, "Russia Unleashed Data-Wiper Malware on Ukraine, Say Cyber Experts," *Guardian*, February 24, 2022, https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts.

d ESET, "ESET Research: Ukraine Hit by Destructive Attacks before and during the Russian Invasion with HermeticWiper and IsaacWiper," March 1, 2022, https://www.eset.com/us/about/newsroom/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/.

e "Case Study: Viasat Attack," CyberPeace Institute, June 2022, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

f "Case Study: Viasat."

g Dennis Schwarz and Brett Stone-Gross, "DanaBot Launches DDoS Attack against the Ukrainian Ministry of Defense," *Zscaler Blog* (blog), Zscaler, n.d., https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense?web_view=true.

h Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft On the Issues, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

i Amanda Macias, Kevin Breuniger, and Chloe Taylor, "Ukrainian Officials Say Nuclear Power Plant Secure after Russian Attack," CNBC, March 3, 2022, https://www.cnbc.com/2022/03/03/russia-ukraine-live-updates.html.

j Charlie Osborne, "CaddyWiper: More Destructive Wiper Malware Strikes Ukraine," ZDNET, accessed April 7, 2025, https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/.

k Computer Emergency Response Team of Ukraine, "Кібератака групи UAC-0035 (InvisiMole) на державні організації України (CERT-UA#4213)," March 18, 2022, https://cert.gov.ua/article/37829.

too. Others argue that Russians wanted to gather intelligence from Ukrainian systems more than disrupt them, that Russia's information-focused troops have been more optimized for propaganda than cyber operations, and that cyber scholars' and pundits' expectations were plain wrong given that Russia wanted to inflict physical violence on Ukraine more than achieve cyber-related effects—necessitating bombs, missiles, and guns over malware, zero days, and DDoS attacks.

In reality, of course, many factors are likely in play at once. Plenty of the above scholars and commentators recognize this multifactorial situation and say it outright (although a few do push a single prevailing explanation for the war's cyber outcomes). However, it's worth explicitly stressing that many factors coexist, in light of occasional efforts to provide reductive explanations for complex wartime activities and effects. Concluding that Russia is no longer a cyber threat, for instance, is wrong. While Ukraine as a country has demonstrated extraordinary will and resilience, and while Ukrainian cyber defenses have been more than commendable, explanations that place the rationale solely on formidable Ukrainian cyber defenses are likewise reductive. Taking such explanations as fact simplifies the many factors involved and can veer analysis and debates away from the policy actions that are still needed, such as continued cyber threat information sharing between the United States and Ukraine.

The above, plausible, evidence-grounded explanations are not mutually exclusive. FSB officers, rife with paranoia, conspiratorialism, and a Putin-pleasing orientation, did indeed grossly misinterpret the situation on the ground in Ukraine in 2022 and fed that bad information to the Kremlin, potentially skewing assessments of cyber options as well.

Interagency competition may very well have undermined, once again, the ability of the FSB, GRU, and SVR to coordinate activities with one another, let alone with the Ministry of Defense and Russian proxies in Belarus, and therefore hampered more effective planning, coordination, and execution of cyber operations. For example, during the war's initial stages, elements of the SVR may very well have sought to technically gather intelligence from targets that GRU- or FSB-tied criminal groups were indiscriminately trying to knock offline or wipe with malware, thrusting uncoordinated activities into tension.

Like in every other country on earth, Russian cyber operators are additionally subject to resource constraints: a hacker spending a day on breaking into a Ukrainian energy company is a hacker not spending time on spying on expats in Germany or setting up a collaboration with a ransomware group. Competition, therefore, not just between agencies—turf wars, budget fights, who gets the primary jurisdiction over Ukraine, and so forth—but within them, over who gets to spend what time and resources targeting which entities, sit within broader Russian government calculi over cyber, military, and intelligence operations. And, among others, Russia's overall strategy did lead to bad moves, as Wilde and others have noted, with limited effect and burning away Russian capabilities (like exploits) in the process. Recognizing these many likely factors will facilitate better analysis of where Russia stands.

The gap between the imagined, all-out "cyber war" and the past three years' reality also begs the question of whether the right metrics were considered in the first place. As much as cyber capabilities are inextricable from modern

intelligence operations, and as much as cyber and information capabilities are embedded throughout militaries around the world, war is obviously about far more than cyber as a domain. But experts studying cyber all day, every day, may fall into the unintentional trap (as anyone can) of having their area of study become the focal point of analysis in a war with many moving pieces and considerations—hence, some of the commentary anticipated Russian destruction of Ukraine to happen through code, compared to a range of military weaponry. Academic theories, moreover, of how cyber conflict will unfold in political science-modeled simulations or think tank war games may similarly fail to map to battlefield realities, such as generalizing how cyber fits into warfare without adequately considering unique contexts in a country like Russia. Layered on top of all this—in the academies, in the media, in the data and artificial intelligence (AI) era—is a frequent desire to quantify everything, too, obscuring the fact that not everything can be effectively, quantifiably measured and that counting up the number of observed Russian cyber operations and scoring them may still not get to the heart of their inefficacy.

Clearly, as US and Western perspectives on Russian cyber power shift with more information and time, it is worth rethinking Russia's future cyber power—not just for how the West can recalibrate its assumptions and size up the threats, but in how the West can prepare to act and respond in the future.

UNPACKING THE (CYBER) NESTING DOLL

The takeaway from comparing predictions and reality shouldn't be that pundits are always wrong or that Russia's cyber operations are considerably less threatening in 2025. Nor should it be that Ukraine is propped up solely by Western government and private-sector cyber defenses, and that Russia is simply waiting to unleash a devastating cyber operation to end it all.

Russia remains a sophisticated, persistent, and well-resourced cyber threat to the United States, Ukraine, and the West generally. This is not going to change anytime soon. Kremlin-spun "crackdowns" on cybercrime (arrests that were little more than public relations stunts), frenetic talk of US-Russia rapprochement, and wishful thinking about Putin's willingness to cease subversive activity against Ukraine do not portend, as some might suggest, that the United States can sideline Russia as a central cyber problem—and focus instead on China.

The Russian government views cyber and information capabilities as key to its military and intelligence operations, and the Kremlin still has one top enemy in its national security sights: the United States. Outside the Russian state per se, a range of ransomware gangs and other hackers in Russia will continue targeting companies, critical infrastructure, and other entities in the United States, Ukraine, and the West, too. There are at least five steps US policymakers and their allies and partners should take to size up this threat—against the full scope of Russia's cyber web and integrating lessons learned so far from Russia's full-out war on Ukraine—and confront it head-on in the coming years.

When assessing the expectations-versus-reality of Russia's wartime cyber operations, distinguish between capabilities and wartime execution. Clearly, Russian offensive cyber activity during its full-on war against Ukraine has not matched up against Western assumptions that envisioned a cyber onslaught that turned off power grids, disrupted water treatment facilities, and blacked out communications. Evaluating how and why Russia did not make this happen is critical to understanding Russia's operational motives, play-by-play planning and coordination between security agencies, targeting interests, and much more. But analysts and media must be careful to avoid thinking that Russia's cyber capabilities themselves are weak. Clearly, when Russian hackers put the pedal to the metal, so to speak—ransomware gangs targeting American hospitals, or the GRU going after Ukrainian phones—they can deliver serious results. A better approach is policymakers and analysts in the United States, as well as in allied and partner countries, breaking out Russia's continued cyber threats across ransomware, critical infrastructure targeting, mobile-device hacking, and so on while pairing the capabilities against where execution could fall short in

practice. Doing so will give a better sense of Russia's cyber strengths and weaknesses—and distinguish between the different components of carrying out a cyber operation.

Widen the circle of analysis to include not just Russian state hackers but the broader Russian cyber web, including patriotic hackers and state-coerced criminals. Focusing Western intelligence priorities, academic studies, and industry analysis mainly on Russian government agencies as the primary vector of Russian cyber power loses the importance of the overall Russian cyber web. Putting the focus mostly on Russian government agencies also loses, as my colleague Emma Schroeder has unpacked in detail, the role that public-private partnerships have played in cyber operations and defenses in the conflict, and the opportunity to assess similar public-private dynamics on the Russian side. Conversely, making sure to consider the roles of government contractors, military universities, patriotic hackers, state-tapped cybercriminals, and other actors as described above should help to fight the temptation to treat all Russian cyber operations as top-down—and illuminate the many ways in which Russia can build capabilities, source talent, and carry out operations against the West. Understanding these actors will allow for better tracking, threat preparation, defense, and, where needed, disruption.

Avoid the trap of assuming Russia can separate out cyber and information issues from other bilateral, multilateral, and security-related topics—maintaining its hostility toward Ukraine while, say, softening up on cyber operations against the United States. Whether the US government can or cannot separate out cyber issues vis-à-vis Russia from other elements of the US-Russia relationship (e.g., trade, nuclear security), Western policymakers should avoid the trap of assuming the Russian government is currently capable, let alone willing, of genuinely and seriously doing the same: separating out its cyber activities from other policy and security issues.

The Russian government has come to view the internet and digital technologies as both weapons that can be wielded against the state and weapons to use against Russia's enemies. In this sense, cyber operations (as well as information operations) are core not just to Moscow's approach to modern security, military activity, and intelligence operations but, perhaps more importantly, to the Kremlin's conceptualization of regime security as well. Paranoia and propaganda about fifth columnists (with, sometimes, one feeding the other), persistent efforts to crack down on the internet in Russia, and a continued belief that Western tech companies and civil society groups are weaponizing the

internet to undermine the Kremlin, mean that the regime will not truly believe it can put "information security" on the sidelines—and that includes not just internet control but cyber operations. Policymakers must go into diplomatic and other engagements with Russia with their eyes wide open.

Continue cyber information sharing about Russia with allies and partners around the world. For years, military and intelligence scholars and analysts have referred to Russia's actions in Georgia, Ukraine, and other former Soviet republics as a "test bed" or "sandbox" for what Russia might do in other countries. It would be a strategic, operational, and tactical mistake to think that Russian cyber operations against Ukraine are just confined to Ukraine and that two-way information sharing with Ukraine about cyber threats is a waste of time and resources. Quite the opposite: Russia's cyber and information activities against Ukraine today can give the United States and its allies and partners critical insights into the types of capabilities and operations that could, and very well might be, carried out against them at the same time or days or months later. Whether hack-and-leak operations designed to embarrass political figures, wiper attacks designed to destroy government databases, espionage operations, or anything in between, having real-time information about Russian cyber threats will only help the United States and its allies and partners better defend their own networks and systems against hacks and attacks.

Invest in cyber defense and in cyber offense where appropriate. Persistent, sophisticated Russian cyber threats to a range of key US and allied and partner systems—military networks, hospitals, financial institutions, critical infrastructure, advanced tech companies, civil society groups—demand continued investments in cyber defense. In addition to information-sharing, the United States and its allies and partners need to continue prioritizing market incentives for companies to enhance cyber defenses along with baseline requirements for essential measures such as multifactor authentication, detailed access controls, robust encryption, continuous monitoring, network segmentation, resourced and empowered cybersecurity decision-makers, and much more. Just as the Russians clearly possess a range of advanced cyber capabilities, any number of recent operations, including against Ukraine, show that Russian operations (like those carried out by many other powers) continue to succeed with basic moves such as phishing emails. The United States and its allies and partners need to continually increase cyber defenses. And, where appropriate, the United States and its allies and partners should ensure the right capabilities and posture to carry out cyber offensive operations—including to preemptively disrupt Russian attacks (the "defend forward" euphemism). As the Kremlin is more paranoid and conspiratorial, the notion of diplomatic talks and establishing cyber redlines is less and less realistic. Active mitigation and disruption of threats, rather than relying too heavily on diplomatic meetings or endless criminal indictments, are together a more feasible approach to protecting US and allied and partner interests against Russian cyber threats in the years to come.

CONCLUSION

Lessons from cyber operations—and about cyber operations and capabilities—from the Russian full-on war against Ukraine will continue to emerge in the coming years. This trickle of information may slowly dissipate some of the "fog of war" surrounding the back-and-forth hacks and shed much-needed light on issues such as coordination and conflict between Russian security agencies in cyberspace.

For now, however, the issue for the United States is clear: Russia remains a persistent, sophisticated, and well-resourced cyber threat to the United States and its allies and partners around the world. The threat stems from a range of Russian actors, and it stands to continue impacting a wide range of American government organizations, businesses, civil society groups, individuals, and national interests across the globe. As wonderful as the idea of cyber détente might be, Putin's paranoia about Western technology, Russian officials' insistence that the internet is a "CIA project" and Meta is a terrorist organization, and military and intelligence interest in conflict and subversion against the West will not evaporate with a wartime ceasefire or a newfound agreement with the United States. These are hardened beliefs and fairly cemented institutional postures that are not going to shift under the current regime.

Rather than dismissing Russia's cyber prowess because of unmet expectations since February 2022, American and Western policymakers must size up the threat, unpack the complexity of Russia's cyber web, and invest in the right proactive measures to enhance their security and resilience into the future.

ACKNOWLEDGEMENTS

The author would like to thank Brian Whitmore and Andrew D'Anieri for the invitation to write this paper and for their comments on an earlier draft. He also thanks Gavin Wilde, Trey Herr, Aleksander Cwalina, Ambassador John Herbst, and Nikita Shah for their comments on the draft.

ABOUT THE AUTHOR

Justin Sherman is a nonresident senior fellow with the Cyber Statecraft Initiative, part of the Atlantic Council tech programs. He is also the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm; an incoming adjunct professor at Georgetown University's School of Foreign Service; a contributing editor at *Lawfare*; and a columnist at *Barron's.* He writes, researches, consults, and advises on Russia security and technology issues and is sanctioned by the Russian Ministry of Foreign Affairs.

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
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Alain Bejjani
Colleen Bell
Sarah E. Beshar
*Karan Bhatia
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
David L. Caplan
Samantha A. Carl-Yoder
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
George Chopivsky
Wesley K. Clark
*Helima Croft
Ankit N. Desai
*Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Stuart E. Eizenstat
Tara Engel
Mark T. Esper
Christopher W.K. Fetzer
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
*Meg Gentle
Thomas H. Glocer
John B. Goodman
Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Robin Hayes
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Karen Karniol-Tambour
*Andre Kelleners
John E. Klein
Ratko Knežević
C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Diane Leopold
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Roger R. Martella Jr.
Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
*Ahmet M. Ören
Ana I. Palacio
*Kostas Pantazopoulos
David H. Petraeus
Elizabeth Frost Pierson
*Lisa Pollina
Daniel B. Poneman
Robert Portman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Laura J. Richardson
Thomas J. Ridge
Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Jeff Shockey
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Melanne Verveer
Tyson Voelkel
Kemba Walden
Michael F. Walsh
*Peter Weinberg
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
*Jenny Wood
Alan Yang
Guang Yang
Mary C. Yates
Dov S. Zakheim

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

**Executive Committee Members*

List as of March 24, 2025

1400 L Street NW, 11th Floor
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org