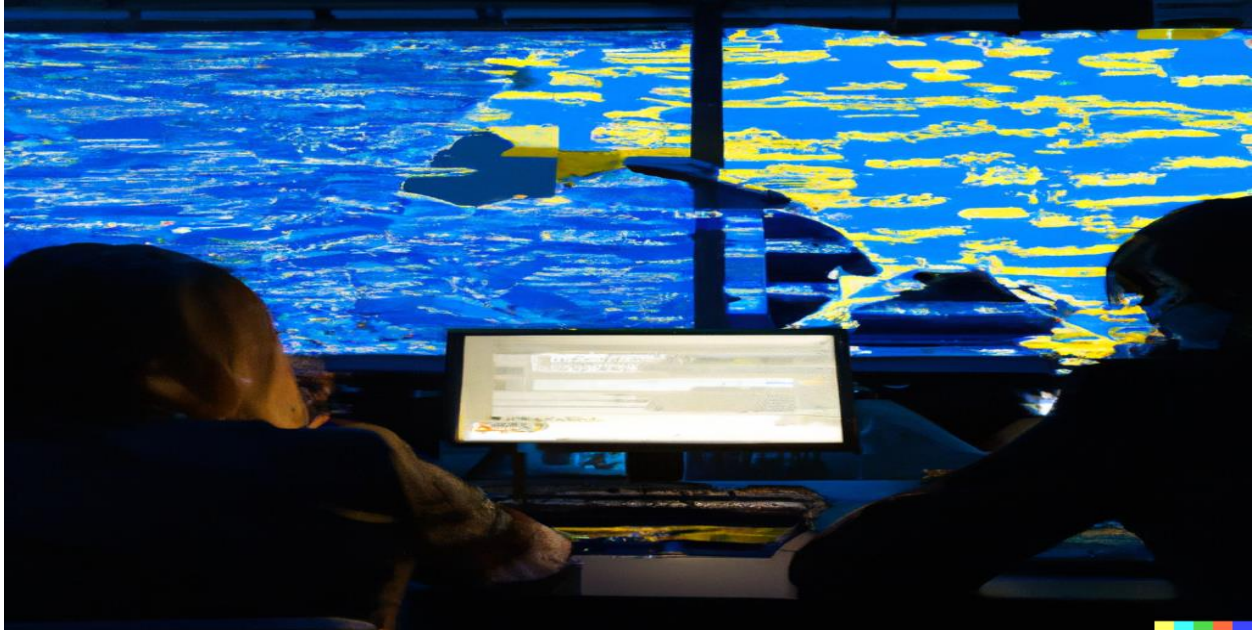


CNA

November 2023



## Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons

Jaclyn A. Kerr

Distribution unlimited  
IOP-2023-U-037223-Final

## Abstract

What lessons can be learned from the early phase of the Ukraine war concerning Russia's capabilities, strategy, and approach in cyberspace? To what extent do these point to broader conclusions about the domain's role during above-threshold military conflict? This article examines Russian use of cyber and information capabilities to influence the course of the Ukraine war, analyzing prior expectations, what is publicly known of wartime realities, potential reasons for disparity between the two, and the distinct and sometimes contradictory take-aways that have been drawn within the analytical community. While the lack of consensus among experts this far into the conflict demonstrates the difficulty of drawing conclusions with incomplete and early evidence, it also indicates a division between analyses focused on evidence of Russian cyber activities versus those focused on questions of strategic impact. It likewise highlights the challenges to strategic learning and adaptation posed by the domain's covert nature.

---

This report is part of a series generously funded by a grant from the Carnegie Corporation of New York. CNA's Occasional Paper series is published by CNA, but the opinions expressed are those of the author and do not necessarily reflect the views of CNA or the official policy or position of the Department of the Navy, the National Defense University, the Department of Defense, or the US government.

Approved for public release: distribution unlimited.


11/22/2023

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

**Cover image:** Created by author using DALL-E software.

This document may contain materials protected by the Fair Use guidelines of Section 107 of the Copyright Act, for research purposes only. Any such content is copyrighted and not owned by CNA. All rights and credits go directly to content's rightful owner.

**Approved by:**



**November 2023**

Colleen McCue, PhD, Acting Research Program Director  
Countering Threats and Challenges Program  
Strategy, Policy, Plans, and Programs Division

# Contents

---

<b>Introduction.....</b>	<b>1</b>
<b>Russia’s Approach to Cyberspace .....</b>	<b>5</b>
A sophisticated threat actor.....	5
Ukraine as “test bed”.....	8
<b>Wartime Expectations and Realities.....</b>	<b>10</b>
Great expectations .....	10
Lackluster realities? .....	12
<b>What Happened: A Bark, but Not a Bite? .....</b>	<b>20</b>
Conflict-specific explanations .....	20
Broader lessons for wartime cyber .....	27
<b>Conclusion: Strategic Adaptation and the Wartime Cyber Debate .....</b>	<b>32</b>
Parsing the wartime cyber debate .....	32
Information, adaptation, and learning.....	35
<b>References.....</b>	<b>37</b>

This page intentionally left blank.

# Introduction

---

Judging by noteworthy headlines and expert analyses, one might be forgiven for some measure of confusion about the cyber domain's role in the first year and a half of Russia's full-scale war with Ukraine. These discussions have run the gamut. The war's cyber dimension has been called a "game changer"<sup>1</sup> and a "turning point for cyberwarfare"<sup>2</sup> that has "transformed the cyber threat landscape."<sup>3</sup> Russian efforts have been referred to as "relentless and destructive,"<sup>4</sup> of "unprecedented magnitude,"<sup>5</sup> "strategic and deliberative,"<sup>6</sup> "aggressive and multi-pronged,"<sup>7</sup> the "most sustained and intrusive cyber-campaign on record,"<sup>8</sup> amounting to "full-on, full-scale

---

<sup>1</sup> Cristina Vanberghen, "Ukraine Marks a Turning Point for Cyberwarfare," *Politico*, Dec. 28, 2022, <https://www.politico.eu/article/russia-ukraine-cyber-invasion-warfare-kremlin-nato/>. Vanberghen is a senior expert at the European Commission.

<sup>2</sup> Vanberghen, "Ukraine Marks a Turning Point."

<sup>3</sup> Google Threat Analysis Group, Mandiant, and Google Trust & Safety, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," Google Report, Feb. 16, 2023; Shane Huntley, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," *Google Updates from Threat Analysis Group*, Feb. 16, 2023, <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/>.

<sup>4</sup> Microsoft Digital Security Unit, "An Overview of Russia's Cyberattack Activity in Ukraine," Special Report: Ukraine, Apr. 27, 2022; Tom Burt, "The Hybrid War in Ukraine," *Microsoft on the Issues (Microsoft Blog)*, Apr. 27, 2022, <https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/>.

<sup>5</sup> David Cattler and Daniel Black, "The Myth of the Missing Cyberwar," *Foreign Affairs*, Apr. 6, 2022, <https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar>.

<sup>6</sup> Microsoft, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft Report, June 22, 2022, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>; Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft on the Issues (Microsoft Blog)*, June 22, 2022, <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.

<sup>7</sup> Huntley, "Fog of War."

<sup>8</sup> Quote from Lindy Cameron, head of Britain's National Cyber Security Centre (NCSC). See "Lessons from Russia's Cyber-War in Ukraine," *Economist*, Nov. 30, 2022, <https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine>.

cyberwar,”<sup>9</sup> even the “world’s first full-scale cyberwar.”<sup>10</sup> Technical reports have pointed to skyrocketing numbers of cyberattacks, both prior to and during the conflict, both on Ukraine and its allies. Ukraine’s government has appealed to The Hague to prosecute Russian cyberattacks as war crimes.<sup>11</sup> Nonetheless, many experts have also described Russian cyberattacks as surprisingly ineffective, as having “fallen flat.”<sup>12</sup> They have characterized Russia as “losing the information war,”<sup>13</sup> and they have debated reasons for the apparent absence of “cyber shock and awe,”<sup>14</sup> referring to cyber as the “dog that didn’t bark.”<sup>15</sup>

This striking lack of a clear consensus over how to interpret the role of cyberspace in Russia’s war with Ukraine stems at least in part from the magnitude of early expectations. Russia is one of the US’s foremost competitors in cyberspace, and it has long demonstrated its willingness to bring its cyber power to bear in efforts to gain desired strategic outcomes, particularly in its “near abroad,” and nowhere more than in Ukraine. For this reason, as intelligence and the gathering of Russian troops on the Ukrainian border in early 2022 drew international attention to the imminent threat of a Russian invasion of its militarily weaker neighbor, many also predicted a particularly catastrophic cyber onslaught—whether in substitute or preparation for, or as a complement to a full-scale invasion. Yet since its invasion of Ukraine, Russia has not

---

<sup>9</sup> Quote from an April 2022 interview with Tom Burt, Microsoft’s vice president of customer security and trust. See Dustin Volz and Robert McMillan, “In Ukraine, a ‘Full-Scale Cyberwar’ Emerges,” *Wall Street Journal*, Apr. 12, 2022, <https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203>.

<sup>10</sup> Yurii Shchychol, “Vladimir Putin’s Ukraine Invasion Is the World’s First Full-Scale Cyberwar,” Atlantic Council, June 15, 2022, <https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-ukraine-invasion-is-the-worlds-first-full-scale-cyberwar/>.

<sup>11</sup> Shannon Van Sant, “Kyiv Argues Russian Cyberattacks Could Be War Crimes,” *Politico*, Jan. 9, 2023, <https://www.politico.eu/article/victor-zhora-ukraine-russia-cyberattack-infrastructure-war-crime/>.

<sup>12</sup> “Why Russia’s Cyber-Attacks Have Fallen Flat,” *Economist*, Dec. 1, 2022, <https://www.economist.com/leaders/2022/12/01/why-russias-cyber-attacks-have-fallen-flat>.

<sup>13</sup> Jeremy Fleming, “The Head of GCHQ Says Vladimir Putin Is Losing the Information War in Ukraine,” *Economist*, Aug. 18, 2022, <https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine>.

<sup>14</sup> Lennart Maschmeyer and Nadiya Kostyuk, “There Is No Cyber ‘Shock and Awe,’” *War on the Rocks*, Feb. 8, 2022, <https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/>; Cattler and Black, “The Myth of the Missing Cyberwar”; and Nick Beecroft, “Evaluating the International Support to Ukrainian Cyber Defense,” *Cyber Conflict in the Russia-Ukraine War Series*, Carnegie Endowment for International Peace, Nov. 3, 2022, <https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322>.

<sup>15</sup> “Cyber-Attacks on Ukraine Are Conspicuous by Their Absence,” *Economist*, Mar. 1, 2022, <https://www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence>; Jelena Vičić and Rupal N. Mehta, “Why Russian Cyber Dogs Have Mostly Failed to Bark,” *War on the Rocks*, Mar. 14, 2022, <https://warontherocks.com/2022/03/why-cyber-dogs-have-mostly-failed-to-bark/>; and Nadiya Kostyuk and Erik Gartzke, “Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine,” *Texas National Security Review* 5, no. 3 (2022), pp. 113–126, <http://dx.doi.org/10.26153/tsw/42073>.

leveraged these capabilities to secure as great a battlefield advantage as many expected. Early reports of their outside-theater subthreshold uses to undermine international support for Ukraine have likewise suggested more limited effect in key theaters than featured in the direst predictions. Perhaps most remarkably, more than a year and a half into the fighting, there is still no clear consensus within and across expert communities as to how the accruing evidence should be assessed.

This article examines Russian use of cyber and information capabilities to influence the course of the Ukraine war by analyzing prior expectations, public knowledge of wartime realities, potential reasons for disparity between the two, and the distinct and sometimes contradictory takeaways that have been drawn to date within the analytical community. What lessons can be learned from the early phase of the Ukraine war concerning Russia's capabilities, strategy, and approach in cyberspace? To what extent do these lessons point to broader possible conclusions about the role of cyber and information operations during direct military conflict? Furthermore, what explains the dramatically different early responses to these significant questions? How can the strategic community make sense of this debate and arrive at usable lessons? Although the lack of consensus among experts this far into the conflict demonstrates the challenges of drawing conclusions with incomplete and early evidence, we suggest that significant preliminary lessons can be drawn by looking at both sides of the debate—understanding the bases of disagreement and elements of validity to each set of claims.

The remainder of the article is divided into four sections. The first section, “Russia’s Approach to Cyberspace,” lays out what has been considered unique about Russia's approach to the domain and how its capabilities and strategy have weighed upon US and Western cyber threat perceptions. This threat includes Russia's significant technical cyber capabilities and demonstrated willingness to use these in targeting critical infrastructure. It also includes unique and surprising uses of cyber-enabled information operations—including the strategic spread of mis- and dis-information—in ways thought to demonstrate democratic vulnerabilities. This discussion specifically addresses how Ukraine has long been a test bed for using various combinations of these tools for apparent political and strategic objectives.

Following this prior understanding of Russia's capacities and strategy, the second section, “Wartime Expectations and Realities,” examines expectations that existed concerning Russia's potential use of its array of cyber capabilities in relation to the war in Ukraine and the extent to which these expectations have been met. This includes both expectations about how such capabilities could be used surrounding military invasion and escalation and also about how they might contribute to ongoing war efforts. We then compare that baseline to what is known of Russia's uses of these capabilities during the war. Although some mismatch with prior predictions is obvious, it also is clear that the domain has played an active and ongoing role in the conflict.

In the third section, “What Happened? A Bark, but Not a Bite,” we assess the disparity between predictions and outcomes, examining possible reasons why Russia’s cyber operations during the war have not proven as effective as some predictions would have suggested. This analysis also provides some clarity as to how different parts of the expert community have rendered such distinct initial findings. We examine prominent arguments that have been promulgated in the outside analytical expert community, both to explain Russia’s underwhelming cyber performance and reasons why the domain overall has proven less critical than imagined to above-threshold warfighting. Although frequently framed as diametrically opposed to the dramatic assessments of Russia’s extensive cyber activities produced by technical and operational experts—often from government, military, or the private sector—most of these arguments focus on assessing strategic effect rather than activity levels, leaving room for mutual compatibility of claims as well as significant misunderstanding.

The concluding section, “Strategic Adaptation and the Wartime Cyber Debate,” draws preliminary conclusions about possible lessons that can be learned at this stage of the war—both specifically about Russia’s cyber capabilities and strategy and, more theoretically, about how cyber and information operations contribute to the course of armed conflict. Despite disagreements on exact strategic merit and effect, Russian use of the cyber domain during the conflict has been extensive. Ukraine has also clearly mounted a tremendous cyber defense, supported by a wide coalition of governmental and private sector partners. However, many questions still exist. We particularly consider the possible takeaways about the influence of Russian cyber activities on escalation dynamics and partnership cohesion and what we can and cannot say based on currently available information. We also suggest that the ongoing lack of consensus concerning the extent and role of cyber conflict in the current war might be indicative of deeper challenges to strategically relevant wartime learning and adaptation in the cyber domain. This will be of ongoing significance in continuing to counter the Russian threat and support Ukraine in the next stage of the war.



# Russia's Approach to Cyberspace

---

Many of the early predictions of Russia's cyber and information dominance in Ukraine built on years of observations concerning Russian operations in cyberspace and expert analysis of the country's underlying capabilities and strategy. Russia had repeatedly been identified as one of the major powers in cyberspace, often engaging in very active and diverse forms of subthreshold aggression against international targets, frequently including targets in both its regional theater and the West. Not only had it demonstrated a willingness to engage in some forms of cyberattacks on critical infrastructure—a form of attack long feared by many Western cyber domain experts for its devastating and escalatory potential—but Russian cyber operations also pioneered innovative cyber-enabled information operations, sowing surprise by targeting the information spheres of other countries through cyberspace.

## A sophisticated threat actor

Western threat perceptions of Russia as a formidable potential adversary in cyberspace have grown significantly from the late 2000s, shaped by a succession of demonstrative events. Analysts observed the many uses of cyber and information techniques by Russian state and state-related actors as well as their frequent combined use with other forms of aggression, most notably covert or subthreshold grey zone forms of conflict, but also during shooting wars. Early attention was drawn, for example, by Russia's use of cyber aggression against neighbors in Estonia (2007),<sup>16</sup> Georgia (2008),<sup>17</sup> and Ukraine (since 2013).<sup>18</sup>

---

<sup>16</sup> Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, May 16, 2007, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>; "Estonia Hit by 'Moscow Cyber War,'" *BBC News*, May 17, 2007, <http://news.bbc.co.uk/2/hi/europe/6665145.stm>; and James Pamment, Vladimir Sazonov, Francesca Granelli, et al., *Hybrid Threats: 2007 Cyber Attacks on Estonia*, NATO Strategic Communications Centre of Excellence, 2019, <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>.

<sup>17</sup> John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, Aug. 12, 2008, <https://www.nytimes.com/2008/08/13/technology/13cyber.html>; David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, Jan. 6, 2011, <https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>; and Sarah P. White, "Understanding Cyberwarfare: Lessons from the Russia-Georgia War," *Modern War Institute*, Mar. 20, 2018, <https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/>.

<sup>18</sup> Associated Press in London, "Ukraine Attacked by Cyberspies as Tensions Escalated in Recent Months," *Guardian*, Mar. 9, 2014, <https://www.theguardian.com/world/2014/mar/09/ukraine-attacked-cyberspies>.

Several high-profile cyberattacks that have hit Western countries have also been attributed to Russian state-backed or criminal actors. These cyberattacks have, for example, included the 2017 NotPetya malware attack, which initially targeted Ukraine but went on to spread globally, impacting international shipping. They also included the 2020 SolarWinds supply chain attack, where compromised software created breaches into at least nine US government agencies, including the Department of Defense and Department of Homeland Security.<sup>19</sup> Going back to at least 2012, hacker groups linked to the Main Intelligence Directorate of the Russian military's General Staff (GRU) and Federal Security Service (FSB) have repeatedly targeted US electric grid and critical infrastructure networks, including gaining unauthorized access to computer networks at nuclear power facilities, utilities, and airports.<sup>20</sup>

Russian criminal hacking groups and hacktivists have often also been linked to international cyber incidents. Although the FSB later arrested some hackers linked to the REvil and DarkSide hacker groups involved in the high-profile ransomware attacks in 2021 on US Colonial Pipeline and on meat production plants, Russia has also utilized quasi-independent hacker groups as “plausibly deniable” proxies in its international cyber and information operations, raising challenges to attribution and accountability.<sup>21</sup>

Russia has often been credited with pioneering novel forms of “subthreshold of armed conflict” and “grey zone” cyber aggression that, while largely covert, can be strategically significant in

---

tensions-computer; Elina Lange-Ionatamishvili, *Analysis of Russia's Information Campaign Against Ukraine*, NATO Strategic Communications Centre of Excellence, 2015; Kenneth Geers, Editor, *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), <https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/>; and Piret Pernik, “The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine,” in *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, ed. Nicu Popescu and Stanislav Secieru, (European Institute for Security Studies, Chaillot Paper No. 148, Oct. 2018).

<sup>19</sup> Kim Zetter, “The Untold Story of the Boldest Supply-Chain Hack Ever,” *Wired*, May 2, 2023, <https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/>; Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, Aug. 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

<sup>20</sup> David E. Sanger, “Russian Hackers Appear to Shift Focus to US Power Grid,” *New York Times*, July 27, 2018, <https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections.html>; Andy Greenberg, “Hackers Tied to Russia's GRU Targeted the US Grid for Years, Researchers Warn,” *Wired*, Feb. 24, 2021, <https://www.wired.com/story/russia-gru-hackers-us-grid/>; and Katie Benner and Kate Conger, “US Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant,” *New York Times*, Mar. 24, 2022, <https://www.nytimes.com/2022/03/24/us/politics/russians-cyberattacks-infrastructure-nuclear-plant.html>.

<sup>21</sup> Gloria Gonzalez, Ben Lefebvre, and Eric Geller, “‘Jugular’ of the US Fuel Pipeline System Shuts Down after Cyberattack,” *Politico*, May 8, 2021, <https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984>; Maggie Miller, “Russia Arrests Hacker in Colonial Pipeline Attack, US Says,” *Politico*, Jan. 14, 2022, <https://www.politico.com/news/2022/01/14/russia-colonial-pipeline-arrest-527166>; and Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2017).

periods of peace as well as hybrid and political warfare. These efforts include Russia's use of cyber-enabled information and influence operations to spread disinformation and seek to influence public opinion, elections, or domestic conflict in third party countries. In the West, a sense of strategic surprise followed revelations of Russia's attempted interference in the 2016 US election and several European elections in the same period, reinforcing a dramatic increase in the West's tendency to perceive Russia as a threatening and powerful cyber adversary with significant domain capabilities and an innovative strategy that posed defensive challenges for democracies in particular.<sup>22</sup>

---

<sup>22</sup> Following Russia's 2014 Crimea Annexation and 2016 interference in the US election, Western analysts sought to explain Russia's distinct approach to the role of information and digital technology in strategy, including within Russia's broader approach to international competition, coercion, and military strategy. While the West tended to approach cyberspace as a narrowly technical domain, Russia's approach was much more holistic, focused on information broadly and not just information technologies and networks. Concepts of "information confrontation" and "information security" incorporated everything from critical networks, infrastructure, and data, to the contents of media productions, social network activity, public perceptions and opinion, and the cognition of leaders. Russian strategic writings stressed the importance of both "information-technical" and "information-psychological" elements of information competition, indicating "information superiority" as crucial in achieving strategic goals, both militarily and otherwise. A widely analyzed 2013 article by Chief of the General Staff of the Russian Federation Armed Forces General Valery Gerasimov suggested that nonmilitary means should play the much larger role (a 4:1 ratio) compared to military methods in the resolution of interstate conflict. Identifying and exploiting vulnerabilities in the "information spaces" of rivals would be critical to achieving desired political and strategic goals in an asymmetric competition with militarily more powerful adversaries.

Writing in 2015, shortly after Russia's novel application of hybrid activities in Ukraine, Dmitry Adamsky described Russia's approach as one of "cross-domain coercion" in which, while "operat[ing] under the aegis of the Russian nuclear arsenal," Russia sought to "manipulate the adversary's perception, to maneuver its decision-making process, and to influence its strategic behavior while minimizing...the scale of kinetic force use." Critical in this was the integration of "non-nuclear, informational, and nuclear capabilities" into "a holistic coercion campaign [to] be used in the pursuit of deterrence and compellence." Following 2016, many commentators discussed the particular vulnerability of democratic societies to the nonmilitary elements of the Russian approach, with Russian use of "cyber-enabled" information operations and influence campaigns seen as drawing on Soviet and pre-Soviet traditions of "reflexive control," "maskirovka," and "active measures," seeking to leverage freedom of expression, media, and protest in other societies to manipulate discourse and sow distrust and conflict. Russia's technical cyber activities targeting critical infrastructure networks also sometimes caused alarm in the West for their potential use as significant cyber-to-kinetic capabilities—and hence also as tools of coercion. Cyberattacks on the Ukrainian power grid in 2015 and 2016 were interpreted by some in the Western strategic community as not only demonstrating a new capability, but as doing so as a form of deterrent signal directed at competitors beyond Ukraine.

See Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," IFRI Security Studies Center, Proliferation Papers 54, Nov. 15, 2015; Elina Lange-Ionatamishvili, "Analysis of Russia's Information Campaign Against Ukraine," NATO Strategic Communications Centre of Excellence (COE), 2015; Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford: Oxford University Press, 2022), pp. 251–272; Jaclyn A. Kerr, "Concept Misalignment and Cyberspace Instability: Lessons from Cyber-Enabled Disinformation," in *Cyberspace and Instability*, ed. Robert Chesney, James Shires, and Max Smeets (Edinburgh: Edinburgh University Press, 2023), pp. 99–126,

## Ukraine as “test bed”

Russia’s use of cyber and information operations in Ukraine have played a noteworthy and persistent role in forming threat perceptions. Ukraine has frequently been described as Russia’s “test bed” for its cyber capabilities, especially since the 2013 EuroMaidan demonstrations and Russia’s 2014 annexation of Crimea and initiation of conflicts in the Donbas and other regions of the country.<sup>23</sup> During that initial crisis and since the beginning of the military conflict in 2014, Russia has used various cyber means against its neighbor to attain the Kremlin’s political and strategic objectives. These means have included various forms of cyber espionage, disruption, destruction, and information and influence campaigns, targeting the Ukrainian government, military, critical infrastructure, telecommunications, elections, and civilian populations.<sup>24</sup> Tools have ranged from spear-phishing and hack-and-leak campaigns to Distributed Denial of Service (DDoS) attacks, and from the release of wiper malware to attacks aimed to shut down parts of the power grid. Notable examples have included the 2014 attempt to sow doubt in the Ukrainian election results by hacking into the Ukrainian Elections Commission, the 2015 and 2016 efforts to sabotage the Ukrainian electric grid causing temporary power outages, and the economic-havoc-wreaking NotPetya malware attack, which affected some 65 countries.<sup>25</sup>

---

<https://edinburghuniversitypress.com/book-cyberspace-and-instability.html>; Valeriy Akimenko and Keir Giles, “Russia’s Holistic Conceptual Framework for Cyber Activity,” in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, ed. Robert Chesney and Max Smeets (Washington, DC: Georgetown University Press, 2023), pp. 173–200; Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); and Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, DC: Georgetown University Press, 2020).

<sup>23</sup> Andy Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar,” *Wired*, June 20, 2017, <https://www.wired.com/story/russian-hackers-attack-ukraine/>; Laurens Cerulus, “How Ukraine Became a Test Bed for Cyberweaponry,” *Politico*, Feb. 14, 2019, <https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/>; and Lionel M. Beehner, Liam S. Collins, and Robert T. Person, “The Fog of Russian Information Warfare,” in *Perceptions Are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations*, ed. Mark D. Vertuli and Bradley S. Loudon (Fort Leavenworth, Kansas: Army University Press, 2018), pp. 31–50.

<sup>24</sup> Keir Giles, “The Next Phase of Russian Information Warfare,” NATO Strategic Communications Center of Excellence (COE), May 2016, <https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176>; Keir Giles, “Handbook of Russian Information Warfare,” Fellowship Monograph No. 9, NATO Defense College, Research Division, Nov. 2016; and Michael Connell and Sarah Vogler, *Russia’s Approach to Cyber Warfare*, CNA, Mar. 2017.

<sup>25</sup> Lennart Maschmeyer, “The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations,” *International Security* 46, no. 2 (2021), pp. 51–90, [https://doi.org/10.1162/isec\\_a\\_00418](https://doi.org/10.1162/isec_a_00418); Maschmeyer and Kostyuk, “There Is No Cyber ‘Shock and Awe.’”

Russia has also made significant use of cyber-enabled information campaigns in its efforts to influence Ukraine's trajectory. Going back to 2014, Russia has strategically deployed narratives to Ukrainian audiences, including being "brother nations" with a shared history, religion, and culture; mistreatment of Russian-speaking communities in Ukraine and fear of supposed Ukrainian Naziism, portraying the elected government in Kyiv as illegitimate and violent "Banderites"; and nostalgia for and possibility of reclaiming the former Soviet greatness.<sup>26</sup> After the downing of the Malaysia Airlines flight MH17 in July 2014, Russian disinformation campaigns promoted multiple different conflicting narratives, an effort broadly seen by the analytical community as seeking to create uncertainty and deflect attention from real attribution.<sup>27</sup>

In addition to targeting Ukrainian citizens, Moscow has also used cyber-enabled information operations in the West as part of its strategy to influence outcomes in Ukraine. Russian disinformation and influence campaigns targeting US and European elections, political decisions, and public opinion have often been viewed primarily as threats to the targeted country's own national security and investigated to trace their domestic effects. But these campaigns have often been utilized in broader efforts to induce regional outcomes, particularly seeking to undermine Ukraine's movement toward Europe and support for the post-EuroMaidan Kyiv government.<sup>28</sup>

---

<sup>26</sup> Lange-Ionatamišvili, "Analysis of Russia's Information Campaign"; Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Institute for the Study of War (ISW), Russia Report I, Sept. 2015.

<sup>27</sup> Snegovaya, "Putin's Information Warfare."

<sup>28</sup> Gavin Wilde and Justin Sherman, "Targeting Ukraine Through Washington," Atlantic Council Issue Brief, Mar. 2022, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/targeting-ukraine-through-washington/>; Jim Rutenberg, "The Untold Story of 'Russiagate' and the Road to War in Ukraine," *New York Times Magazine*, Nov. 2, 2022, <https://www.nytimes.com/2022/11/02/magazine/russiagate-paul-manafort-ukraine-war.html>.

# Wartime Expectations and Realities

---

How have these prior understandings of Russia as a threat actor in cyberspace matched with what has been seen in the actual conflict in Ukraine? What were the predictions of the expert community going in about Russia's use of cyberspace and about the domain's role in the war more broadly? And to what extent have observed realities met with these—sometimes significant—expectations?

## Great expectations

Prior to the outset of Russia's full-scale invasion of Ukraine on February 24, 2022, expectations in the West concerning the role of the cyber domain in the conflict were shaped by two concurrent considerations. One was the stark understanding of Russia's cyber capabilities, strategic innovativeness in cyberspace, and willingness to utilize these for maximal effect within Ukraine in particular. Based on these understandings, expectations were high that the domain would be employed ruthlessly, leveraging both traditional cyber capabilities and cyber-enabled information campaigns, combined with military operations within theater and used to target and coerce Ukraine's partners abroad.

The other factor shaping expectations was a broader set of assumptions concerning the cyber domain's potential uses and utility in above-threshold conflict, particularly when utilized by a major cyber power with little concern about humanitarian effects and targeting a state with less sophisticated cyber capabilities. As *New York Times* reporting noted during the first week of the war, "[M]ost early tabletop exercises about a Russian invasion started with overwhelming cyberattacks, taking out the internet in Ukraine and perhaps the power grid."<sup>29</sup> Although precise expert predictions here varied, many believed that several prior cyber confrontations which had occurred during peacetime and grey zone conflicts had tamped down on the domain's most devastating uses, preventing actors from utilizing maximally devastating effects such as major cyber-to-kinetic attacks on critical infrastructure. In a full-scale war, the gloves would be off, so more escalatory uses might follow.

Combined, these Western threat perceptions about Russia's role as a powerful malicious cyber actor and the cyber domain's potentially catastrophic role in war contributed to some stark predictions about the role the cyber domain was likely to play in a full-scale war in Ukraine.

---

<sup>29</sup> David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled into Ukraine, So Did Malware. Then Microsoft Entered the War," *New York Times*, Feb. 28, 2022, <https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html>.

Some experts noted concerns about Russia’s potential use of cyberattacks even prior to or in substitute for an armed attack on its neighbor. These concerns explain how electric grid shutdowns during cold weather or attacks on the banking sector or other government systems and communication networks could be used in combination with stepped-up disinformation campaigns to destabilize the economy and cause panic and social unrest.<sup>30</sup> Experts pointed to long-running campaigns already targeting many government agencies which could be expanded. Their efforts could undermine the government of Ukrainian president, Volodymyr Zelensky, either prompting a desired regime change without invasion or as a pretext for one. For this, Russia could leverage false-flag operations and criminal proxy actors to retain a pretext of deniability.

Others warned of Ukraine’s likely vulnerability to extreme forms of cyberattack, whether in preparation of the battlefield or, later, as part of an all-out invasion and war. Technical cybersecurity experts pointed to particular susceptibilities given the extent to which Ukraine’s grid and other infrastructure were partly built under the Soviet system and were still using legacy software or updating with Russian parts. Russian hackers had already been exploiting vulnerabilities in these systems for years and were thought to “understand every linkage in the design—and most likely have insiders who can help them.”<sup>31</sup> In addition to potential attacks on the power grid, government systems, and key economic sectors, during above-threshold war, Russia could use the cyber domain to launch crippling cyber-to-kinetic attacks, equivalent to armed attacks, causing explosions, floods, toxic exposures, and other potentially catastrophic effects on civilian populations. Russia could also use the cyber domain to actively target Ukraine’s warfighting capabilities, including takedowns of Ukrainian wartime command and control systems and undermining defensive military operations, as well as “left-of-bang” attacks on weapons systems that would render them inoperable.

Russia’s presumed expertise in the combined use of cyber and information campaigns was another area that could be particularly detrimental to Ukraine during wartime, potentially undermining support for defensive efforts or further stoking irredentist pro-Russia sentiments among some populations. The aggressor would bring years of experience manipulating discourse and catalyzing resentments in the region combined with boots-on-the-ground support.

Overall, these arguments suggested that Russia could wield its cyber capabilities for highly coercive and militarily influential effects to achieve strategic advantages both in the lead-up to

---

<sup>30</sup> Jason Healey, “Preparing for Inevitable Cyber Surprise,” *War on the Rocks*, Jan. 12, 2022, <https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/>; David E. Sanger and Julian E. Barnes, “US and Britain Help Ukraine Prepare for Potential Russian Cyberassault,” *New York Times*, Dec. 20, 2021, <https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.html>.

<sup>31</sup> Sanger and Barnes, “US and Britain Help Ukraine.”

and during a war with Ukraine. And Ukraine would not be Russia's only target. As Russia appeared to have demonstrated in prior efforts, it could simultaneously leverage its cyber and information capabilities as tools of deterrence and subthreshold coercion and influence against Ukraine's erstwhile supporters or potential allies in the West and elsewhere.<sup>32</sup> This led some to predict significant Russian cyberattacks on Western banking sectors as retaliation for sanctions or the possible leveraging of penetration into critical infrastructure targets for pronounced deterrent signaling to ward off further Western engagement in the conflict.<sup>33</sup>

## Lackluster realities?

So has the cyber domain played a significant role in the war as expected? Has Russia lived up to its reputation as a fierce cyber threat actor? Arguments on these questions in the first year and a half of the war have been remarkably bifurcated and reveal perhaps as much about the organizational ecology of cyber expertise as they do about the cyberattacks under discussion. On one hand, the opening months of the war saw a panoply of public-facing headlines and scholarly reports noting the relative absence of Russia's dreaded cyber or information warfare

---

<sup>32</sup> Samantha Raphelson, "Report: Russian Hackers Had The Ability To Shut Down U.S. Power Plants," NPR, Mar. 16, 2018, <https://www.npr.org/2018/03/16/594371939/u-s-accuses-russia-of-cyberattacks-on-energy-infrastructure>; Bruce Schneier, "An Example of Deterrence in Cyberspace," *Schneier on Security*, June 7, 2018, [https://www.schneier.com/blog/archives/2018/06/an\\_example\\_of\\_d.html](https://www.schneier.com/blog/archives/2018/06/an_example_of_d.html); Jason Healey, "Not The Cyber Deterrence the United States Wants," *Council on Foreign Relations Blog*, June 11, 2018, <https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants>; and David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), pp. 223–226.

<sup>33</sup> Sean Lyngaas and Phil Mattingly, "US Officials Prep Big Banks and Utilities for Potential Russian Cyberattacks as Ukraine Crisis Deepens," CNN Politics, Feb. 18, 2022, <https://www.cnn.com/2022/02/18/politics/treasury-banks-russia-cyber-meeting/index.html>; Mengqi Sun and Richard Vanderford, "U.S. Banks Are Prepared for Russia Sanctions, but Concerns Grow About Potential Hacks," *Wall Street Journal*, Feb. 24, 2022, <https://www.wsj.com/articles/u-s-banks-are-prepared-for-russia-sanctions-but-concerns-grow-about-potential-hacks-11645743246>; Owen Walker and Imani Moise, "Banks on Alert for Russian Reprisal Cyber Attacks on Swift," *Financial Times*, Mar. 15, 2022, <https://www.ft.com/content/a2bdba3b-f1dd-4c9f-a0de-9fff6e744e4>; Nicole Sganga, "'It's Coming': President Biden Warns of 'Evolving' Russian Cyber Threat to U.S.," CBS News, Mar. 21, 2022, <https://www.cbsnews.com/news/russia-cyber-attack-threat-biden-warning/>; Maggie Miller, "Biden's Options If Russia Hacks U.S. Infrastructure," *Politico*, Apr. 20, 2022, <https://www.politico.com/news/2022/04/20/biden-russia-hacks-00026384>; Cybersecurity and Infrastructure Security Agency (CISA), "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," *Cybersecurity Advisory*, May 9, 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>; and Scott Jasper, "The Risk of Russian Cyber Retaliation for the United States Sending Rockets to Ukraine," *Council on Foreign Relations Blog*, June 15, 2022, <https://www.cfr.org/blog/risk-russian-cyber-retaliation-united-states-sending-rockets-ukraine>.



capabilities.<sup>34</sup> At the same time, reports from major private and public sector cybersecurity institutions repeatedly highlighted the upsurge in cyber activity, sometimes referring to the conflict as marking a turning point in the role and nature of cyberwar.<sup>35</sup> While technical and operational cybersecurity experts from military and private sector organizations discussed the herculean defensive efforts required to blunt a massive onslaught amounting to the “most active ‘cyberwar’ ever seen,” then, much of the outside analytical community proffered reasons why Russia’s cyber domain efforts were not more palpable, constituting a “dog that hadn’t barked.”

Although seemingly contradictory on first blush, we will argue that both sets of arguments have some degree of validity. Understanding the distinct starting points and objectives for their analyses will be critical for informing later lessons to be taken from the war and its ramifications for cyber strategy. But before turning to examine likely explanations for these marked differences in analysis from leading experts in different parts of the cybersecurity community, we look at what is known about the cyber dimension of the Ukraine war.

As several reports stress, *a great deal* of cyber activity has occurred. This activity began well in advance of the full-scale invasion on February 24, 2022. Russian cyber operations in Ukraine had ramped up considerably in the lead-up to the war. One piece of this was an increase in Russian reconnaissance activity in Ukrainian networks that began during 2021, including by the Foreign Intelligence Service (SVR)-linked group APT29 (also known as Cozy Bear or Nobelium). Microsoft later reported that “[b]y Mid-2021, Russian actors were targeting supply chain vendors in Ukraine and abroad to secure further access not only to systems in Ukraine but also to NATO member states.”<sup>36</sup> These efforts were accompanied in early 2022 by increased attempts to disrupt Ukrainian systems and services, including across communications, energy, financial, education, and public administration sectors. The prewar period saw defacement attacks on government and university websites, spear-phishing campaigns targeting the energy sector, and DDoS attacks on the Ukrainian Ministry of Defense and the Ukrainian banking sector. Information campaigns during the lead-up to the war sought to create a false *casus belli*, portraying Ukraine as a rights abuser and a violator of arms control conventions

---

<sup>34</sup> See for example Rafal Rohozinski, “Ukraine’s Missing Cybergeddon,” *CIGI Online*, Centre for International Governance Innovation, Mar. 5, 2022, <https://www.cigionline.org/articles/ukraines-missing-cybergeddon/>; “Why Russia’s Cyber-Attacks Have Fallen Flat,” *Economist*, 2022; Kostyuk and Erik Gartzke, “Why Cyber Dogs Have Yet to Bark.”

<sup>35</sup> See for example Vanberghen, “Ukraine Marks a Turning Point”; Shchyhol, “Vladimir Putin’s Ukraine Invasion Is the World’s First Full-Scale Cyberwar”; Microsoft Digital Security Unit, “An Overview of Russia’s Cyberattack Activity in Ukraine”; Microsoft, “Defending Ukraine”; Volz and McMillan, “In Ukraine, a ‘Full-Scale Cyberwar’ Emerges”; Google, et al., 2023; Huntley, “Fog of War”; and CISA, “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.”

<sup>36</sup> Burt, “The Hybrid War.”

that was led by extremist nationalists.<sup>37</sup> A series of destructive wiper malware attacks targeted Ukrainian government, financial, energy, information and communication technology (ICT), agriculture, and nonprofit sectors in January and February, including the Foxblade wiper attacks carried out on the eve of the February 24th invasion by the same Russian Military Intelligence (GRU)-linked group, GRU Unit 74455 or Sandworm, which had launched the 2017 NotPetya attack.<sup>38</sup> This attack was later described by Microsoft as the first cyberattack of the war, one that targeted 19 “government and critical infrastructure entities across Ukraine.”<sup>39</sup>

Russian aggression in cyberspace stepped up further as the war began. During the first days of the conflict, Russia sought to disrupt Ukrainian command and control abilities and public communications. Some campaigns also showed a cross-domain coordination of effects. On February 24, 2022, as Russian forces invaded Ukrainian territory, a Russian cyberattack on Viasat satellite modems shut down satellite communications over Ukraine and part of Europe, also creating spillover effects on German wind turbine systems.<sup>40</sup> A series of attacks through March further disrupted internet access, temporarily taking down three internet service providers: Triolan, Vinasterisk, and Ukrtelecom.<sup>41</sup> Though SpaceX's delivery of Starlink terminals to Ukraine early in the war reinforced communications, these were also quickly

---

<sup>37</sup> Matthias Schulze and Mika Kerttunen, “Cyber Operations in Russia’s War Against Ukraine,” Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, SWP Comment no. 23, Apr. 17, 2023, doi:10.18449/2023C23.

<sup>38</sup> Several different data-wiping malware were deployed on Ukrainian networks, including the Whispergate and Foxblade wipers. See Herbert Lin, “Russian Cyber Operations in the Invasion of Ukraine,” *Cyber Defense Review*, 2022; Schulze and Kerttunen, “Cyber Operations in Russia’s War”; Cyber Peace Institute, “Attack Details,” *Cyber Attacks in Times of Conflict*, accessed Sept. 2023, <https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details>.

<sup>39</sup> Microsoft Digital Security Unit, “An Overview of Russia’s Cyberattack Activity.”

<sup>40</sup> This attack, which used the AcidRain wiper malware to remotely erase ground-based modems and routers associated with broadband satellite internet access through the KA-SAT satellite network, not only disrupted Ukrainian communications during the invasion, but also took down civilian internet service for thousands of Ukrainians as well as thousands of satellite internet subscribers in Germany, France, Hungary, Greece, Italy, and Poland. The attack also affected more than 5,800 wind turbines in Germany. The attack was later attributed to Russia, with EU and Five Eyes countries releasing public statements on May 10, 2022 that linked the attack and several others involving wiper malwares to the GRU. See Cyber Peace Institute, *Case Study: CyberPeace Institute, Case Study: Viasat*, <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat>; Matt Burgess, “A Mysterious Satellite Hack Has Victims Far Beyond Ukraine,” *Wired*, Mar. 23, 2022, <https://www.wired.com/story/viasat-internet-hack-ukraine-russia/?redirectURL=%2Fstory%2Fviasat-internet-hack-ukraine-russia%2F>; Christian Vasques and Elias Groll, “Satellite Hack on Eve of Ukraine War Was a Coordinated, Multi-Pronged Assault,” *Cyberscoop*, Aug. 10, 2023, <https://cyberscoop.com/viasat-ka-sat-hack-black-hat/>; and Patrick Howell O’Neill, “Russia Hacked an American Satellite Company One Hour Before the Ukraine Invasion,” *MIT Technology Review*, May 10, 2022, <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>.

<sup>41</sup> Lin, “Russian Cyber Operations”; Cyber Peace Institute, “Attack Details.”

subjected to disruption attempts by hacking and jamming.<sup>42</sup> A March 1 cyberattack on media outlets brought down a major broadcasting network on the same day that missiles targeted and destroyed the Kyiv television tower.<sup>43</sup> By late April, Microsoft had documented 237 operations carried out against Ukraine by at least six different Russia-aligned actors, including destructive attacks, disruptions, intelligence gathering, and the spread of disinformation. By July, the attempted use of eight separate Russian malware programs—targeting 48 Ukrainian government agencies and enterprises—had been detected, amounting to two to three such attacks per week. Microsoft’s June 2022 report noted that these “ongoing destructive attacks themselves have been sophisticated and more widespread than many reports recognize.”<sup>44</sup> In August 2022, the Computer Emergency Response Team of Ukraine reported over 1,123 cyberattacks in the first six months of the war, a threefold increase in frequency.<sup>45</sup>

Russian cyber operations have continued as a high-tempo and evolving dimension of the conflict into the war’s second year.<sup>46</sup> Some analysis during this period has stressed both Russia’s ongoing assertiveness and continuing innovation in cyberspace.<sup>47</sup> A February 2023

---

<sup>42</sup> Walter Isaacson, “‘How Am I in This War?’ The Untold Story of Elon Musk’s Support for Ukraine,” *Washington Post*, Sept. 7, 2023, <https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/>; Kate Duffy, “Elon Musk Says Russia Has Stepped Up Efforts to Jam SpaceX’s Starlink in Ukraine,” *Business Insider*, May 11, 2022, <https://www.businessinsider.com/elon-musk-spacex-russia-ramps-up-efforts-jam-starlink-ukraine-2022-5>; Kate Duffy, “A Top Pentagon Official Said SpaceX Starlink Rapidly Fought Off a Russian Jamming Attack in Ukraine,” *Business Insider*, Apr. 22, 2022, <https://www.businessinsider.com/spacex-starlink-pentagon-russian-jamming-attack-elon-musk-dave-tremper-2022-4>; and Lin, “Russian Cyber Operations.”

<sup>43</sup> Kate Conger and David E. Sanger, “Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds,” *New York Times*, Apr. 27, 2022, <https://www.nytimes.com/2022/04/27/us/politics/russia-cyberattacks-ukraine.html>.

<sup>44</sup> Microsoft Digital Security Unit, “An Overview of Russia’s Cyberattack Activity”; Smith, “Defending Ukraine”; and Kenneth Geers, “Computer Hacks in the Russia-Ukraine War,” *Def Con 30*, Aug. 11, 2022, <https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/>.

<sup>45</sup> Schulze and Kerttunen, “Cyber Operations in Russia’s War.”

<sup>46</sup> An April 2023 European Cyber Conflict Research Initiative (ECCRI) report commissioned by the UK’s National Cyber Security Centre (NCSC), for example, points to an “unprecedented” “volume of Russian-attributed or supported cyberattacks occurring in Ukraine” with Russian operators “act[ing] with remarkable speed and flexibility...sustaining an unprecedented operational tempo.” See National Cyber Security Centre, “New Analysis Highlights Strength of Ukraine’s Defence Against ‘Unprecedented’ Russian Offensive,” Apr. 20, 2023, <https://www.ncsc.gov.uk/news/new-analysis-eccri-highlights-ukraine-defence-against-russian-offensive>; and Taylor Grossman, Monica Kaminska, James Shires, and Max Smeets, “The Cyber Dimensions of the Russia-Ukraine War,” Workshop Report, European Cyber Conflict Research Initiative (ECCRI), Apr. 20, 2023, <https://eccri.eu/events/the-cyber-dimensions-of-the-russia-ukraine-war/>.

<sup>47</sup> In a May 2023 interview, Yurii Shchyhol, the director of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP, also known as *Derzhspetsvvyazok*), described continuously changing Russian cyberattacks into the second year of the war, with attackers adapting to seek out vulnerabilities, and

Google report noted Russian state linked actors' continued "aggressive, multi-pronged" and strategic efforts in cyberspace targeting Ukraine and its supporters.<sup>48</sup> The report pointed to an increase in the use of destructive attacks on Ukrainian government, military, and civilian targets, with a focus on public services, critical infrastructure, and utilities. It also indicated significant cyber operations targeting NATO countries, including spear-phishing and ransomware. As Clint Watt observed in a March 2023 blog, Russia has made technical and tactical adaptations, including development of new malware, new techniques such as the use of social media to market pirated exploitable software and spear-phishing campaigns targeting governments and emergency response organizations in Europe.<sup>49</sup> Since the beginning of the war, Russia had deployed nine new families of wiper malware and two new types of ransomware, using these "against more than 100 government and private sector Ukrainian organizations." This deployment included the ransomware "Prestige," which had been used in October 2022 in both Ukraine and Poland.<sup>50</sup> Microsoft also reported stepped-up Russian cyber espionage in 2023, including efforts that have targeted government agencies or other organizations in at least 17 European countries. More recent Microsoft reporting also indicates tracking of a new GRU-linked Russian actor since February 2023, Cadet Blizzard, which has been targeting organizations in Europe and Latin America, particularly in NATO countries providing military aid to Ukraine.<sup>51</sup>

Cyber-enabled information and influence campaigns also ramped up with the war. These campaigns have targeted audiences in Ukraine, the West, the Global South, and Russia itself. They have sought to undermine confidence in the Ukrainian government, influence populations to oppose pro-Ukraine policies, fragment the international coalition of support for Ukraine, and maintain domestic support within Russia for the war effort.<sup>52</sup> In keeping with its

---

evidence of increasing unity of effort across hacker groups. See Daryna Antoniuk, "Ukraine's Cyber Chief on the Ever-Changing Digital War with Russia," *The Record: Recorded Future News*, May 21, 2023, <https://therecord.media/ukraine-ssscip-yurii-shchychol-interview>.

<sup>48</sup> Google et al., 2023.

<sup>49</sup> Clint Watts, "Is Russia Regrouping for Renewed Cyberwar?," *Microsoft on the Issues (Microsoft blog)*, Mar. 15, 2023, <https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center/>.

<sup>50</sup> The other, Sullivan, was deployed only in Ukraine in November 2022. See Watts, "Is Russia Regrouping."

<sup>51</sup> The group uses stolen credentials to gain access to peripheral servers, customizes off-the-shelf tools, and uses "living off the land" techniques to hide in legitimate network traffic, making it challenging to detect. See Tom Burt, "Ongoing Russian Cyberattacks Targeting Ukraine," *Microsoft on the Issues (Microsoft blog)*, June 14, 2023, <https://blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyberattacks-ukraine-cadet-blizzard/>.

<sup>52</sup> Christopher Bronk, Gabriel Collins, and Dan Wallach, "Cyber and Information Warfare in Ukraine: What Do We Know Seven Months In?," Baker Institute Issue Brief, Baker Institute for Public Policy, Rice University, Sept. 6, 2022, <https://doi.org/10.25613/69E1-WZ16>; Vasques and Groll, "Satellite Hack on Eve."

prior approaches, Moscow has used a mix of techniques in its attempts to shape media and information environments, often amplifying divisive local issues and voices and targeting tailored disinformation and narratives for specific audiences. Russia-linked actors have used known state-backed media outlets alongside networks of covert accounts and coordinated inauthentic activity on social media platforms, hack-and-leak operations, falsified imagery, disruption, or censorship of media outlets, and the deliberate spread of advantageous narratives.<sup>53</sup> These efforts have promoted narratives focused on negatively portraying Ukrainian refugees and stoking resentment toward them in host countries. They have pushed concerns about deteriorating standards of living, high energy prices, food insecurity, and crime, drawing connections to Western pro-Ukraine policies.<sup>54</sup> Other narratives have blamed Ukraine as the source of modern-day fascism and promoted distrust of Western media as biased or untruthful.<sup>55</sup>

Research tracking Russian information campaigns in the first year and a half of the conflict demonstrate these efforts have reached well beyond Ukraine, seeking to influence the internal politics and public attitudes about the conflict in third countries. A February 2023 report by the Atlantic Council DFRLab shows the Kremlin to have been aggressively engaging in information operations to shape opinions about the war in the developing world, including Africa and Latin America.<sup>56</sup> Other research shows efforts to sow distrust and undermine collaboration across countries in Europe and NATO, including those engaged directly in support for the Ukrainian war effort. A Recorded Futures report from July 2022 traced Russian campaigns aiming to create or exacerbate divisions in the Western coalition that support Ukraine, doing so both by engendering domestic discontent with political leadership's support for Ukraine within Western countries and by sowing distrust and tensions between states. These efforts included campaigns to evoke tension between NATO countries, with RT stories, for example, repeatedly stressing extreme political divisions between Poland and Germany or insoluble disagreements between Poland and the Baltics versus Germany, France, and Turkey,

---

<sup>53</sup> Recorded Future, "Russian Information Operations Aim to Divide the Western Coalition on Ukraine," Cyber Threat Analysis: Russia, Insikt Group, July 7, 2022, <https://www.recordedfuture.com/russian-information-operations-divide-western-coalition-ukraine>; Digital Forensic Research Lab (DFRLab), "Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine," Atlantic Council, Feb. 22, 2023; and Huntley, "Fog of War."

<sup>54</sup> An "unverified analytical note" from the Russian Federal Security Service (FSB) reportedly intercepted by Ukraine's Security Service in June 2022 called for targeting the "European Community" with messages about the influx of Ukrainian refugees leading to "deteriorating living standards." See Recorded Future, "Russian Information Operations."

<sup>55</sup> Recorded Future, "Russian Information Operations"; Digital Forensic Research Lab (DFRLab), "Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression against Ukraine," Atlantic Council, Feb. 22, 2023.

<sup>56</sup> DFRLab, "Narrative Warfare."

suggesting radically different stakes or positions in relation to the war. In Poland, one of Ukraine's most ardent supporters that has taken in large numbers of refugees, Russian actors have sought to leverage historical grievance narratives and ethnic tensions.<sup>57</sup> A hack-and-leak campaign in November 2022 published an alleged Telegram correspondence of Moldovan politicians to suggest that "officials [had] rigged elections or [had] been installed improperly in their positions." This effort apparently aimed to undermine anti-corruption officials and bolster the pro-Russia opposition.<sup>58</sup>

Russia has also taken extreme efforts to control and influence domestic discourse and opinion as well as targeting Russian diaspora communities. Since the war, these efforts have included an unprecedented crackdown on independent media and free expression within Russia and encouraging more active displays of support.<sup>59</sup> They have also included significant efforts to manipulate discourse through covert information operations. A February 2023 report by Google found that most covert information operations disrupted by the company on "Google product surfaces" had been focused on maintaining Russian domestic support for the war.<sup>60</sup> These operations spiked particularly during the initial prewar buildup, the invasion, and the September 2022 troop mobilization. DFRLab's research also shows influence campaigns targeting Russian emigrant communities abroad, where individuals who left Russia prior to the war might be vulnerable to "pro-Kremlin messaging." These campaigns have involved "pro-Russia rallies in Europe[and] the defacement of tourist attractions with pro-war symbols" and have encouraged "conflicts between Russian diaspora and Ukrainian refugees."<sup>61</sup>

Despite this abundance of cyber activity, many experts analyzing the cyber dimensions of the war have depicted the domain as playing a relatively minor role in the overall conflict, especially considering Russia's prior reputation as a cyber threat actor. They have pointed to a lack of influential battlefield effects on the order expected in prewar analyses. No nationwide power outage was caused instantaneously by cyberattack, with no complete takedown of the banking sector. The most obvious influence campaigns within Ukraine appeared ham-fisted and ineffective. When Russia wanted to shut off internet services, troops took over internet service provider (ISP) facilities.<sup>62</sup> When they wanted to take down the power grid or affect

---

<sup>57</sup> Recorded Future, "Russian Information Operations."

<sup>58</sup> Lily Hay Newman, "Security News This Week: A Destabilizing Hack-and-Leak Operation Hits Moldova," *Wired*, Nov. 19, 2022, <https://www.wired.com/story/moldova-leaks-google-privacy-settlement-world-cup-apps/>.

<sup>59</sup> Jaclyn A. Kerr, "Runet's Critical Juncture: The Ukraine War and the Battle for the Soul of the Web," *SAIS Review of International Affairs* 42, no. 2 (2022), pp. 63–84, <https://doi.org/10.1353/sais.2022.0011>.

<sup>60</sup> Huntley, "Fog of War."

<sup>61</sup> DFRLab, "Narrative Warfare"; DFRLab, "Undermining Ukraine."

<sup>62</sup> Lin, "Russian Cyber Operations."

other critical infrastructure, they used shelling and explosives. With the abundance of overtly visible kinetic activity and the relative sparsity of equally overt battlefield cyber effects, analysis has examined why Russia has not more obviously overpowered Ukraine in cyberspace or why, more generally, the role of the cyber domain has not appeared as decisive as those of other domains and technologies.

Given the wide variety of documented Russian cyber and cyber-enabled operations since the war began, what explains the relatively deflationary rhetoric about the domain's role? During the first days of the war, some of this rhetoric could be justified based solely on a lack of awareness: evidence of the extent of Russian cyber operations came late relative to awareness of other more visible aspects of the conflict. A continuing issue is also likely to be the covert nature of cyber operations and the relative scarcity of public information about ongoing events.<sup>63</sup> As a result, awareness of adversarial activities and how they are being defeated or defended against is likely to be much greater among those directly involved in the defensive collaboration, whether in Ukraine, in partner governments and militaries, or in private sector firms assisting in areas of Ukrainian cyber defense. However, the researchers and experts penning outside commentaries questioning Russia's effective use of the domain or what it shows about the role of cyberspace in above-threshold warfare are hardly neophytes to the field who lack awareness of these information disparities. Rather, in some cases, they are addressing distinct questions—not about the extensive role of cyber operations in the conflict, but about the exact nature of that role and what it shows about actor capabilities, strategy, and the specific roles of the cyber domain in above-threshold warfare.

---

<sup>63</sup> The lagging and incomplete nature of public information about ongoing cyber activities can complicate inference concerning ongoing dyadic exchanges between rival actors. As JD Work and Richard Harknett have explained, this can potentially result in distorted interpretations of the strategic dynamics. Although available information might suggest an “episodic” pattern of discrete attacks and counterattacks, for example, these might be just “fleeting glimpses” of ongoing cyber campaigns involving more continuous engagement between actors. See JD Work and Richard Harknett, “Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges,” Atlantic Council Issue Brief, July 22, 2020, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/>.

# What Happened: A Bark, but Not a Bite?

---

Prominent arguments about the role of cyberspace in the Ukraine war mostly focus on the domain's impact, not its activity level. The arguments suggest, by one measure or another, that the domain has not been as influential as expected. It may very well have been immensely active, but it has not been decisive. The explanations advanced largely take one of two forms: the first provides conflict-specific reasons, which have to do with reevaluating the capabilities and strategies of the respective actors—Russia, Ukraine, support for Ukraine—or they consider unique features of this conflict. The other set of explanations have focused on the role of cyberspace in above-threshold conflicts writ large. These explanations use the Ukraine war as a case against which to examine broadly applicable theories about the domain's wartime role. Both sets are thought-provoking and significant inquiries, and they have produced a variety of potentially crucial though sometimes contradictory insights.

## Conflict-specific explanations

Conflict-specific arguments have focused attention on explaining the relative performance of Russia and Ukraine in the cyber and information dimensions of the war. These arguments have included large amounts of commentary on Russia's apparent underperformance. Commentators point to the absence of obvious major battlefield effects stemming from Russian cyber operations as indication of a lack of adequate preparation and relatively weak integration of cyber campaigns into joint operations. Some of these failures are viewed as symptomatic of systemic problems with the Russian military preparation for the conflict, including secrecy, plans only for a short and victorious conflict, and poor logistics and joint operational coordination. It takes quite a bit of advanced planning and detailed intelligence to ensure that more complex cyber operations are effective, and Russian cyber operators were hamstrung by some of the same problems that also beset the invading forces during the early weeks of the conflict. Although they had had some operations ready on the eve of the invasion, the Russian leadership's inadequate planning for a longer war had reduced the cyber planning



horizon, forcing rapid improvisation of a type that did not play to the country's potentially vast cyber advantage.<sup>64</sup>

Other arguments have gone further, suggesting Russian cyber capabilities had in fact been overestimated in prewar assessments. The failures to realize worst threat scenarios were a result of this disparity and not merely a result of systemic problems affecting the Russian military. Although past Russian cyber operations had indeed showcased sophisticated and potentially devastating capabilities relevant to warfighting scenarios, such as the ability to remotely shut down portions of the electric grid or do physical damage to critical infrastructure, these abilities had never been demonstrated at scale, and the assumption that the proofs of concept were indeed scalable in a wartime scenario may have overestimated Russian resources and capacity. Other arguments have pointed to specific ideas of breakdown in Russian cyber capabilities because of their organization structures or strategic focus.<sup>65</sup> Possible sources of unforeseen weakness include inadequate coordination as well as competition between units across the GRU, SVR, and FSB, internal reprisals against

---

64 James A. Lewis, "Cyber War and Ukraine," Center for Strategic and International Studies (CSIS), June 16, 2022, <https://www.csis.org/analysis/cyber-war-and-ukraine>; Jon Bateman, *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Cyber Conflict in the Russia-Ukraine War Series, Carnegie Endowment for International Peace, Dec. 16, 2022, <https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657>; Gavin Wilde, *Cyber Operations in Ukraine: Russia's Unmet Expectations*, Cyber Conflict in the Russia-Ukraine War Series, Carnegie Endowment for International Peace, Dec. 12, 2022, <https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607>; and Jon Bateman, Nick Beecroft, and Gavin Wilde, *What the Russian Invasion Reveals About the Future of Cyber Warfare*, Cyber Conflict in the Russia-Ukraine War Series, Carnegie Endowment for International Peace, Dec. 19, 2022, <https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667>.

<sup>65</sup> Jon Bateman suggests that "Moscow's cyber effectiveness" has been "constrained [by] inadequate Russian cyber capacity, [and] weakness in Russia's non-cyber institutions" as well as Ukraine's strong defensive efforts. In particular, he points to the necessarily high tempo of cyber operations during wartime, Moscow's efforts to simultaneously maintain or escalate its cyber campaigns against both Ukrainian and global targets, and its failure to "fully [leverage] cyber criminals as an auxiliary force against Ukraine" as factors contributing to a strain on Russian cyber resources and capacity during the war. Bateman argues that intelligence collection—not destructive or disruptive attacks ("fires")—has "likely been the main focus of Russia's wartime cyber operations in Ukraine." Gavin Wilde explains this as a natural result of "Russia's premier offensive cyber capabilities" being "housed within agencies focused on intelligence and subversion [...] rather than combined-arms warfare." These include units within the FSB, GRU, and the SVR. Bateman suggests that even "cyber-derived intelligence" appears to have had limited effect on Russian warfighting, however, with little evidence, for example, that this has improved Russian artillery or missile targeting. He argues that Moscow's ineffective use of cyber intelligence could be a result of Russia's war not being waged in a "precise, intelligence-driven manner." Wilde suggests that Russian cyber and information strategy may have overemphasized slow, long-term processes of "subversive erosion" (such as cyber influence and disruption campaigns) over the building of a mature, integrated "warfighting support apparatus." See Bateman, *Russia's Wartime Cyber Operations*; Wilde, *Cyber Operations in Ukraine*; and Lin, "Russian Cyber Operations."

organizations blamed for past failings, too much reliance on proxy actors outside of normal chain of command, and a strategic overemphasis on mixed cyber and information operations.<sup>66</sup>

Other prominent arguments draw attention primarily to extraordinary Ukrainian cyber successes, as opposed to Russian failures. Ukraine—with the help of outside partners and experts from the private sector, Western governments, and civil society—has mounted extremely strong cyber defenses. These efforts ramped up both prior to and after the invasion; Ukraine had already been improving its cyber defensive capabilities since 2014 because of ongoing Russian cyberattacks. The country had been building partnerships with outside experts, receiving training and assistance to improve cyber resilience. It had been working to harden the cyber defenses of likely targets, monitor key networks to detect intrusions, and improve rapid response and mitigation capacities.<sup>67</sup> The Ukrainian government had been working to develop mature cyber organizations, including the establishment of a cyber police

---

<sup>66</sup> Andrei Soldatov and Irina Borogan make the point that, despite significant technical talent and a wide range of cyber actors, Russia lacks a “unified cyber command” to allocate roles and coordinate action under military command structures. Instead, decision-making often occurs through political processes conducted at the level of the presidential administration, with Russia’s Security Council serving as a crucial power conduit. This has sometimes led to significant political shakeups undermining existing organizations. They trace evidence of the “decimation” of the FSB Counterintelligence Service’s Information Security Center (TsIB) in the aftermath of the 2016 US election interference, with officials being blamed for getting caught by the US intelligence community, leading to an internal reprisal. Soldatov and Borogan further note that “there is no strict division of labor between the agencies in the cyber domain,” whether military versus nonmilitary or foreign versus domestic. Rather, the “FSB and SVR have attacked military targets,” and the GRU has targeted domestic nonmilitary targets such as journalists and opposition figures. They point to a degree of fungibility between organizations that might lead to resource or talent competition, with different Russian cyber organizations sometimes recruiting from the same talent pools, as well as leveraging relationships with overlapping actors in the private sector, academic institutions, and the criminal cyber underground. Wilde suggests that Russia’s strategic focus has potentially also influenced the organizational developments, with Russian cyber and information strategy overemphasizing slow, long-term processes of “subversive erosion” (such as cyber influence and disruption campaigns) over the building of a mature, integrated, “warfighting support apparatus.” Even after the Russian Ministry of Defense’s 2017 acknowledgement of the creation of a trained cadre of “Information Operations Troops” (*Voyska Informatsionnykh Operatsiy*, VIO) under military command, as Akimenko and Giles explain, the limited publicly available information suggests that these do not constitute a unified cyber command equivalent and that their primary focus is on “propaganda, disinformation, psychological manipulation, and strategic communications.”

See Andrei Soldatov and Irina Borogan, *Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities*, Center for European Policy Analysis (CEPA), Sept. 8, 2022, <https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/>; Wilde, *Cyber Operations in Ukraine*; Maria Latsinskaya, Alexander Bratersky, and Ignat Kalinin, “*Rossiia vvela voyska v internet*” [Russia Sent Troops to the Internet], *Gazeta.Ru*, Feb. 22, 2017, [https://www.gazeta.ru/tech/2017/02/22\\_a\\_10539719.shtml](https://www.gazeta.ru/tech/2017/02/22_a_10539719.shtml); Damien Sharkov, “Russia Announces ‘Information Operations’ Troops With ‘Counter-Propaganda’ Remit,” *Newsweek*, Feb. 22, 2017, <https://www.newsweek.com/russia-announces-information-operations-troops-counter-propaganda-559656>; and Akimenko and Giles, “Russia’s Holistic Conceptual Framework.”

<sup>67</sup> Lewis, “Cyber War and Ukraine.”

force and of cyber capabilities under the military general staff and intelligence agencies.<sup>68</sup> In the opening days of the war, the Ministry of Digital Transformation recruited the so-called “IT Army of Ukraine,” a pro-Ukraine crowdsourced hacking effort.<sup>69</sup> Volunteers were provided with regularly updated lists of Russian targets—from media outlets to banks to government websites—which can be subjected to DDoS outages, hack-and-leak, graffiti, or other cyber operations. Minister Mykhailo Fedorov also led Ukrainian efforts to call on the global technology private sector for assistance in Ukraine’s war effort, whether by calling for companies to withdraw from Russia or by securing their stepped-up support for Ukraine’s cyber defense and communications needs.

Some experts suggest that Ukraine’s cyber defense has proved surprisingly successful because of robust networks of collaboration with private sector and governmental partners. Western companies, including Microsoft, Amazon, Google, ESET, SpaceX, and Recorded Future, provided significant forms of assistance relevant to the cyber dimensions of the conflict. They helped to secure digital data and records in the cloud and away from vulnerable servers, assisted in the identification of new vectors of attack, and identified and examined new forms of malware or sources of network outages. They also helped to provide more robust communications, sensor, and data analysis capabilities. Governmental partners have also been critical. Prior to Russia’s February 24, 2022 invasion, the United States and United Kingdom governments were both reported to have “deployed cyberwarfare teams to assist Ukrainian forces in developing better cyber defenses.”<sup>70</sup> Western information sharing and intelligence support has also been

---

<sup>68</sup> Nadiya Kostyuk and Aaron Brantly, “War in the Borderland Through Cyberspace: Limits of Defending Ukraine Through Interstate Cooperation,” *Contemporary Security Policy* 43, no. 3 (2022), pp. 498–515, <https://doi.org/10.1080/13523260.2022.2093587>.

<sup>69</sup> Since 2019, President Volodymyr Zelensky’s administration had been building a new ministry, the Ministry of Digital Transformation, that was established with the goal of making government services digitally accessible and improving transparency and responsiveness. This new ministry came to play a leading role in coordinating the national response to Russian cyberattacks.

<sup>70</sup> Kostyuk and Brantly, “War in the Borderland.” In November 2022, Nick Beecroft documented a variety of forms of international support that had been contributed to Ukraine’s cyber defense, including support from the US, UK, EU, and NATO. This included collaboration and support for network defense operations, capacity building, and the sharing of threat intelligence. US Cyber Command has explained how “US joint forces, in close cooperation with the government of Ukraine, conducted defensive cyber operations alongside Ukrainian Cyber Command personnel” in the lead-up to Russia’s invasion “as part of a wider effort to contribute to enhancing the cyber resiliency in national critical networks.” A US Cyber Command public affairs article from November 2022 recounts how, in December 2021, the command deployed a “hunt forward” team of US Navy and US Marine Corp cyber operators to Ukraine to work alongside Ukrainian cyber experts to “[hunt] for malicious cyber activity on Ukrainian networks” as Russian troops were massing on the border. They stayed until days before the invasion, “work[ing] closely with the Ukrainian partners, and assist[ing] in analyzing the attacks while also sharing that information with US domestic interagency and industry partners for homeland defense.” As US Marine Corp Major

reported to have played a vital role.<sup>71</sup> Many experts also point to the potential involvement of Western persistent engagement and forward defense operations capable of interfering with the activities of Russian threat actors responsible for attacks on Ukraine. Such tactics had famously been used against Russia's Internet Research Agency in 2018 to disrupt their election interference operations, and a similar approach could prove vital in assisting Ukraine's defense against Russia's most capable cyber actors.<sup>72</sup>

Similar debates have played out concerning the information dimensions of the conflict. Numerous arguments have sought to explain why Russian cyber-enabled information operations have not been as dominant as expected, appearing to have little impact on the battlefield and limited observed effects so far on the most critical international support for Ukraine's defense. In Ukraine and its partners, Russian information campaigns are described as broadly unsuccessful. Some Russian propaganda narratives have been characterized as ham-fisted, with limited potential relevance or plausibility to audiences within the theater. Perhaps Russia failed to recognize the extent of Ukrainian patriotism and will to fight early in the conflict. The Russians failed to apprehend the extent to which populations they were targeting already had set beliefs, making them less vulnerable to the types of narrative messages Russia was attempting to leverage.

Many observers have indicated that the Kremlin's greatest successes in the information environment have in fact been at home within Russia and in the Global South. They point to the ubiquitous propaganda and pervasive crackdown on all forms of independent media and antiwar opposition within Russia. But even at home, questions arise concerning the Kremlin's lack of control over the various conflicting and critical pro-war patriotic narratives of the so-

---

Sharon Rollins has written, the "in-country mission" then "transitioned...to remote operations...continuing to remotely support Ukraine in its cyber defenses."

See Asian News International, "US, UK Send Cyberwarfare Teams to Ukraine Amid Concerns Over Russia," Business Standard, Dec. 20, 2021, [https://www.business-standard.com/article/international/us-uk-send-cyberwarfare-teams-to-ukraine-amid-concerns-over-russia-121122100134\\_1.html](https://www.business-standard.com/article/international/us-uk-send-cyberwarfare-teams-to-ukraine-amid-concerns-over-russia-121122100134_1.html); Sanger and Barnes, "US and Britain Help Ukraine"; Beecroft, "Evaluating the International Support"; Cyber National Mission Force Public Affairs, "Before the Invasion: Hunt Forward Operations in Ukraine," US Cyber Command, Nov. 28, 2022, <https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/>; and Sharon Rollins, "Defensive Cyber Warfare Lessons from Inside Ukraine," US Naval Institute, *Proceedings* 149, no. 6 (2023), p. 1,444, <https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine>.

<sup>71</sup> US Cyber Command, for example, made valuable indicators of cyber compromise available to support Ukrainian cyber defenses. See Bronk, Collins, and Wallach, "Cyber and Information Warfare."

<sup>72</sup> Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *New York Times*, Feb. 26, 2019, <https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html>.

called “Z universe.”<sup>73</sup> In addition, the issue of outright coercion and use of force being substituted for more nuanced information manipulation mechanisms exists.<sup>74</sup> These developments have led some experts to ask if Russia was ever as capable in the information domain as it was given credit for being. Perhaps Western analysts indulged in threat inflation, mistaking the widespread abundance of Russian information campaigns for evidence of superior capability and impact.

For other analysts, the difference again lies in Ukraine’s superior defensive achievements and in the assistance it has gathered. From the war’s onset, President Volodymyr Zelensky and his administration have shown significant media savvy and audience awareness, beginning with Zelensky’s February 25th video posting from Kyiv announcing that he and his team were still in the capital and Russia’s attempted regime decapitation had failed.<sup>75</sup> The Ukrainian government has taken considerable actions to strengthen information resilience and counter Russian information operations. It has established new institutions to this end, including “the Ministry of Information Policy, the National Council on Television and Radio Broadcasting, and the National Security and Defense Council.”<sup>76</sup> It has worked with government, private-sector, and open-source intelligence community partners to track, expose, and debunk Russian disinformation, leveraging intelligence and analytical support to rapidly address false narratives.<sup>77</sup> It has collaborated with civil society to support fact-checking efforts such as StopFake and VoxCheck, also launching new education and public awareness initiatives to promote media literacy and digital resilience among Ukrainian citizens. New laws and legal actions have been used to address some Russian efforts to infiltrate the Ukrainian media space.<sup>78</sup> At the same time, Ukraine has itself made very effective use of messaging, using nightly official broadcasts, far-reaching diplomatic engagements, and campaigns across social media and other digital platforms to disseminate pro-Ukrainian narratives, both casting Russia in an at-times comically disparaging light and eliciting sympathy and support from outside audiences. As one September 2022 report explained, “In information operations, Ukraine has

---

<sup>73</sup> The potential significance of this shortcoming and the Kremlin’s continuing effort to better control pro-war narratives has of course been showcased in June–August 2023 by the insurrection and later fate of the Wagner mercenary group’s head, Evgeny Prigozhin. See Victor Davidoff, “Reading the Tea Leaves of Russia’s Pro-War ‘Z- Universe,’” *Moscow Times*, Oct. 14, 2022, <https://www.themoscowtimes.com/2022/10/13/reading-the-tea-leaves-of-russias-pro-war-z-universe-a79078>.

<sup>74</sup> Since February 2022, many journalists, activists, and protesters have been imprisoned in Russia. Large numbers have also left the country to continue their work in exile, setting up new independent media outlets or rights groups from abroad. See Kerr, “Concept Misalignment.”

<sup>75</sup> Schulze and Kerttunen, “Cyber Operations in Russia’s War.”

<sup>76</sup> DFRLab, “Narrative Warfare.”

<sup>77</sup> Geers, “Computer Hacks.”

<sup>78</sup> DFRLab, “Narrative Warfare.”

been able to effectively turn everything from leaked, unsecure Russian communications to video of anti-armor ambushes into a narrative of triumph over a hapless opponent.”<sup>79</sup>

Thus, many of the arguments about the role of the cyber domain during the first year and half of the war have focused on relative capabilities or performance of the respective offensive and defensive efforts. But there are still other arguments that suggest an absence of decisive Russian cyber victories is not merely a result either of Russian failure or Ukrainian success. Instead, it is simply a matter that Russia has so far decided not to utilize its full suite of cyber capabilities to the extent that it might have—but that it still could.<sup>80</sup> Explanations offer various possible reasons why Russia would have chosen to hold off: Russian forces want to use the internet and the infrastructure themselves, for example, for espionage, for information operations, for their own communications, or to preserve them for later when they govern the territory. Perhaps Russia lacks suitable targets for some large-scale effect because some of the key critical infrastructure is not networked and therefore is harder to access and target through cyber means than by missiles. Some operational aims might be difficult to achieve through cyber means because of timing, since it takes time to exploit systems.<sup>81</sup> Risks of inadvertent escalation also might be a concern, whether horizontal or vertical. A case in point of this would be the wind turbines in Germany that were affected by the Viasat attack; perhaps Russia has wanted to avoid worse uncontrolled consequences of attacks that could involve other parties in the conflict.

Another possibility highlighted by some observers is that the Kremlin has held some of its more consequential cyber and information capabilities in reserve for later.<sup>82</sup> High-end cyber capabilities could be used as a deterrent, possibly, or could be useful for escalation dominance at a later stage in the conflict. Likewise, as the war drags on, there is increasing awareness of potential longer-term vulnerabilities to persistent Russian information operations aimed less at evincing rapid battlefield effects or quick swings of public opinion than at leveraging the slowly growing war fatigue to undermine support for Ukraine’s war efforts among key partners in the long term.

---

<sup>79</sup> Bronk, Collins, and Wallach, “Cyber and Information Warfare.”

<sup>80</sup> John Sakellariadis and Maggie Miller, “Ukraine Gears Up for New Phase of Cyber War with Russia,” *Politico*, Feb. 25, 2023, <https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429>; Chris Krebs, “The Cyber Warfare Predicted in Ukraine May Be Yet to Come: As Russia’s Economy Deteriorates, the Red Lines Keeping Its Cyber Capabilities in Check May Evaporate,” *Financial Times*, Mar. 20, 2022, <https://www.ft.com/content/2938a3cd-1825-4013-8219-4ee6342e20ca>.

<sup>81</sup> This explanation, of course, collapses somewhat into the former argument about Russia’s failures because of inadequate preparations. As we shall see, it also fits with some of the more general arguments about the cyber domain’s role in above-threshold conflict.

<sup>82</sup> Jeff Seldin, “US Bracing for Bolder, More Brazen Russian Cyberattacks,” VOA News, Mar. 7, 2023, <https://www.voanews.com/a/us-bracing-for-bolder-more-brazen-russian-cyberattacks/6992938.html>.

## Broader lessons for wartime cyber

The previous sections, of course, are very specific to the current conflict. But some scholars and analysts have pointed to broader lessons that might be drawn based on observations from the Ukraine war. They suggest that conflict-specific arguments alone are insufficient to explain the limited visibility or indecisive effect of cyber operations in the conflict. In their April 2022 *Foreign Affairs* article, “The Myth of the Missing Cyber War,” NATO officials David Cattler and Daniel Black<sup>83</sup> have argued that it was incorrect to have expected some form of “cyber shock and awe,” and that such overt visibility will never be an appropriate basis for evaluating the actual effect of cyber campaigns—even if they are quite successful.<sup>84</sup> Several scholars and analysts have gone further, arguing that even after accounting for significant Russian cyber aggression during the war, generalizable lessons about the cyber domain’s fundamental attributes and limitations can be drawn from Russia’s apparent failure to decisively affect strategic outcomes through cyber means against an ostensibly weaker opponent.

One such area of strategically significant theoretical arguments has concerned the offense-defense balance in cyberspace. Some expert commentators have pointed to lessons concerning the domain’s offense-defense balance and the possibility to successfully defend against a capable and determined adversary. Conventional wisdom has long held that cyberspace favors the attacker.<sup>85</sup> Although many recent Western strategic adaptations have sought to rectify this imbalance, Ukraine’s relatively successful cyber defense could constitute a significant shift, demonstrating an effective model and underscoring the significance of long-term investment in defensive measures (such as target hardening and rapid detection and reaction capabilities), and of building public-private, whole-of-government, and international mechanisms of defense

---

<sup>83</sup> David Cattler is NATO Assistant Secretary General for Intelligence and Security. Daniel Black is Principal Analyst at NATO’s Cyber Threat Analysis Branch.

<sup>84</sup> Cattler and Black argue that “the lack of overwhelming ‘shock and awe’ in cyberspace has led to the flawed presumption that Russia’s cyber-units are incapable, and even worse, that cyber-operations have offered Russia no strategic value in its invasion of Ukraine.” But they suggest this is the wrong metric of evaluation, one which “poses an unrealistic test of strategic value” because “no single domain of operations has an independent, decisive effect on the course of war.” Despite various shortcomings, they argue, “Russian cyber-units successfully attacked a range of targets in accordance with Russia’s war plans.” See Cattler and Black, “The Myth of the Missing Cyberwar.”

<sup>85</sup> Thoughtful counterarguments concerning the theoretical possibilities for the domain’s offense-defense balance have been made. In a 2016 *International Security* article, for example, Rebecca Slayton argued that the offense-defense balance need not necessarily favor attackers, in part because of the expense in time and resources required to prepare the most high-end, effective cyberattacks. But the constant drumbeat of apparently successful cyberattacks has perpetuated an understanding of the domain as favoring offense—bringing with it many implications for the likelihood of first strikes and escalation. See Rebecca Slayton, “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment,” *International Security* 41, no. 3 (2016–17), pp. 72–109, <https://www.jstor.org/stable/26777791>.

cooperation.<sup>86</sup> The leveraging of new artificial intelligence-based cyber defense tools has also been noted for its contribution to early detection and response capabilities. Such a shift in perceived and achievable offense-defense balance, if it endures, could mark a dramatic change in the domain's strategic characteristics and uses, as has been seen historically, for example, in the development of the air domain.

Others have argued that the war demonstrates more fundamental differences between the cyber domain and conventional warfighting domains, showing that cyber and kinetic capabilities are not always fit for the same purposes. Although conventional military operations are often focused on occupying territory, seizing resources, terrorizing civilian populations, and ultimately reducing the opponent's ability to fight, some cyber experts see the domain's greatest obvious utility being as a tool for espionage, sabotage, and subversion.<sup>87</sup> These uses for intelligence gathering, covert operations, and political influence have shown considerable value in subthreshold and grey zone forms of conflict, and most agree can also have critical roles during wartime.<sup>88</sup> Beyond these "informational" roles, however, some analysts question whether it is appropriate to consider offensive cyber operations as directly suited for achieving military objectives such as coercion and warfighting. Some point to the Russian need to amass troops in pre-war coercive signaling as indicative that a cyber buildup alone was not even expected to be sufficient for this task.<sup>89</sup> Others have suggested cyber

---

<sup>86</sup> Lewis, "Cyber War and Ukraine"; Schulze and Kerttunen, "Cyber Operations in Russia's War"; and Bateman, *Russia's Wartime Cyber Operations*.

<sup>87</sup> Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012), pp. 5–32, <https://doi.org/10.1080/01402390.2011.608939>; Kostyuk and Gartzke, "Why Cyber Dogs Have Yet to Bark"; Lin, "Russian Cyber Operations"; and Schulze and Kerttunen, "Cyber Operations in Russia's War."

<sup>88</sup> An important recent debate in the scholarly literature focuses on whether cyber conflict might be best understood as an "intelligence contest" as opposed to a form of warfare. Seeing intelligence activities primarily through the prism of "war" might foster inappropriate expectations of "death and destruction" while limiting strategic understanding. As Joshua Rovner has laid out, writing in the immediate aftermath of the SolarWinds breach, seeing cyber competition as an intelligence contest would imply that the domain has five primary competitive uses: "to collect more and better information relevant to a long-term political competition"; "to exploit that information for practical gain"; "to undermine the adversary's morale, institutions, and alliances"; "to disable adversary intelligence capabilities through sabotage"; and "to pre-position assets for future collection in the event of a conflict." This is, of course, both a debate about the domain's universal characteristics and, also necessarily, about how it is understood and used by specific actors. Writing in the same edited volume, authors Valeriy Akimenko and Keir Giles argue that the "intelligence contest" frame does not fully capture the breadth of Russian cyber and information operations—"a combined campaign designed to accomplish a wide range of missions, from tactical intelligence gathering to actions intended to achieve major strategic goals." See Joshua Rovner, "The Elements of an Intelligence Contest," in *Deter, Disrupt, or Deceive* (2023), pp. 17–42; Akimenko and Giles, "Russia's Holistic Conceptual Framework for Cyber Activity," in *Deter, Disrupt, or Deceive* (2023), pp. 173–200.

<sup>89</sup> Lewis, "Cyber War and Ukraine"; Lin, "Russian Cyber Operations."



capabilities cannot substitute for or complement conventional kinetic capabilities involved in fighting for control over territory.<sup>90</sup>

A central question here is whether cyber operations are equally capable of achieving the kinds of effects most crucial for advancing desired strategic outcome in above-threshold conflict, whether through degrading an opponent's critical warfighting abilities, or by undermining their resolve and will to fight. Partly, this is a question of sheer destructive capacity and ability to achieve sudden and surprising effects: although high-end offensive cyber operations might be theoretically capable of similar destructive effects to kinetic operations such as bombing, artillery fire, or missile strikes, a lot depends on where, when, and under what conditions those effects can be achieved. This is likely to be contingent both on the particular state actor's cyber force organization and on more fundamental attributes of the domain.<sup>91</sup> Although some experts hold that cyberspace has a fundamental predisposition to surprise attack,<sup>92</sup> others have argued that the domain's core characteristics make successful integration of high-end destructive attacks particularly difficult during open warfare, in which contexts conventional capabilities will usually prove more fit for purpose.<sup>93</sup>

The ability to attrit an adversary's warfighting capabilities with cyberattacks partly depends on *what* can be targeted, *how quickly*, and in what sorts of *combined operations*. Can cyber operations be used to directly undermine an adversary's essential warfighting tools, such as weapons and command and control communications systems?<sup>94</sup> Can they undermine

---

<sup>90</sup> Kostyuk and Gartzke argue, for example, that cyber capabilities are inherently informational tools most useful for competition over control of information such as beliefs and data—not territory. See Kostyuk and Gartzke, "Why Cyber Dogs Have Yet to Bark."

<sup>91</sup> The manner in which a state's cyber forces are integrated under chain of command could prove significant here, with divisions between the use cases of cyber and conventional capabilities being further magnified by organizational differences. Where states have relied heavily upon nonmilitary or proxy actors to maintain greater deniability in their grey zone cyber activities, for example, the same loose affiliation structures might prove problematic to implementing careful battle plans under a tight chain-of-command.

<sup>92</sup> Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review* 3, no. 4 (2020), pp. 30–53, <http://dx.doi.org/10.26153/tsw/10962>; Healey, "Preparing for Inevitable Cyber Surprise."

<sup>93</sup> Maschmeyer and Kostyuk, for example, argue that the strategic value of cyber operations will usually be modest relative to the use of conventional weapons because of limits in the achievable speed, intensity, and control with which these operations can be conducted—particularly in wartime settings. See Maschmeyer and Kostyuk, "There Is No Cyber 'Shock and Awe.'"

<sup>94</sup> Critical military logistics should also be considered for this list. If weapons, fuel, or troops cannot get to where they need to be on time, for example, this can have major deleterious effects on warfighting capability. See Bradley Martin, D. Sean Barnett, and Devin McCarthy, *Russian Logistics and Sustainment Failures in the Ukraine Conflict*, RAND, Jan. 1, 2023, [https://www.rand.org/pubs/research\\_reports/RRA2033-1.html](https://www.rand.org/pubs/research_reports/RRA2033-1.html); Marcos A. Melendez III, Michael E. O'Hanlon, and Jason Wolff, "America Can't Afford to Ignore the Logistics Triad," Brookings Institution, July 2023, <https://www.brookings.edu/articles/america-cant-afford-to-ignore-the-logistics-triad/>.

munitions production or lead to significant combatant casualties? Can these effects be synchronized to create strategic opportunities or cause *faits accomplis*?<sup>95</sup> Some experts suggest that cyber operations cannot be as readily used against certain categories of targets or as easily integrated into joint operational plans. Because of uncertainties in outcome and timing, cyber operations might not hit targets with the degree of precision and certainty required for integration into tightly interdependent fast-moving operational plans.<sup>96</sup> This could be particularly true of some classes of high-value targets that are relevant to degrading an

---

<sup>95</sup> More analyses to date have focused on Russia's ability to achieve strategically relevant effects through cyber means than on that of Ukraine or other actors. In considering broader lessons about the cyber domain's potential for strategic impact on the course of above-threshold conflict, however, the domain's relevant uses by all parties to the conflict must be taken into account. One example of a potentially significant cyber event early in the war was the disruption of Belarusian rail services by an activist hacker group calling themselves the "Cyber Partisans" with the stated goal of "'slow[ing] down the transfer' of Russian soldiers that are entering Ukraine" and "buy[ing] additional time for Ukrainians to resist Russia's assault[.]" As RAND scholars have pointed out, poor logistics contributed to the failure of Russia's initial attempted *coup de main* in Kyiv "that created the conditions for a prolonged war" rather than a rapid Russian *fait accompli*. While many factors likely contributed to that failure, future analyses of the cyber domain's role in the conflict will necessarily need to consider cyber logistical interference that either was conducted at key moments to stymie strategically significant Russian operations or that could have been. Any continuing capacity to interfere with the function of the Belarusian railway system could also prove relevant in relation to Russia's purported transfer of tactical nuclear weapons to its ally.

See Martin, Barnett, and McCarthy, *Russian Logistics and Sustainment Failures in the Ukraine Conflict*; Shalini Nair, "Belarus Hackers Attack Train Systems to Disrupt Russian Troops," *Railway Technology*, Mar. 1, 2022, <https://www.railway-technology.com/news/belarus-hackers-attack-train-systems/>; Andy Greenberg, "Why the Belarus Railways Hack Marks a First for Ransomware," *Wired*, Jan. 25, 2022, <https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/>; The Associated Press, "Bluffing or Not, Putin's Declared Deployment of Nuclear Weapons to Belarus Raises Tensions," *AP News*, July 27, 2023, <https://apnews.com/article/russia-ukraine-war-belarus-putin-nuclear-3bc2aefef4ee6b4478c81ae76bebdd4e>; Hans Kristensen and Matt Korda, "Russian Nuclear Weapons Deployment Plans in Belarus: Is There Visual Confirmation?," Federation of American Scientists, June 30, 2023, <https://fas.org/publication/russian-nuclear-weapons-deployment-plans-in-belarus-is-there-visual-confirmation/>; and BELZHD Live, "*Порядок ввоза российского ядерного оружия в Беларусь*" [Procedure for Importing Russian Nuclear Weapons into Belarus], *BELZHD Info*, Community of Railway Workers of Belarus (SZhB), June 27, 2023, <https://belzhd.info/military-transportation/poryadok-vvoza-rossijskogo-yadernogo-oruzhiya-v-belarus/>.

<sup>96</sup> Herbert Lin asks to what extent powerful cyber capabilities appear to influence a state's coercive or warfighting capacity—and thus its ability to affect political outcomes (by the Clausewitzian other means). He argues that "neither Russian cyber operations nor troops were successfully brandished to achieve a *coercive* effect on Ukraine" [italics added]. Regarding *warfighting*, he finds "no reports of cyberattacks against Ukrainian weapons systems or military command and control systems per se" and suggests an underlying generalizable reason that he argues could potentially extend beyond the conflict in Ukraine—namely that "cyberattacks are less effective against targets in the category of 'absolutely, positively must be destroyed or disabled with high confidence and certainty or on a certain timetable.'" See Lin, "Russian Cyber Operations."

adversary's ability to fight. In many cases, it might simply be quicker, less expensive, and more effective to use conventional weapons.<sup>97</sup>

These limitations would help to explain the Russian wartime focus on conducting offensive cyber operations against civilian targets—particularly civilian critical infrastructure. Although these targets might be less protected than critical military systems, they still have the potential for significant destructive effects. Attacks need not be as tightly synchronized; other battlefield operations need not depend on their success and timing. Though attacks on such targets do little to affect an adversary's raw warfighting capability, they might be presumed to affect civilian morale—and ultimately the nation's continuing will to fight. But even here, experts point to the relatively limited effect of attempted destructive cyberattacks on critical infrastructure in Ukraine compared to the much more consequential effects of conventional kinetic strikes.<sup>98</sup> Furthermore, even where a state's cyber power is brought to bear effectively on nonmilitary targets, researchers suggest these sorts of attacks can do little to advance long-term strategic goals, neither significantly degrading adversary warfighting capabilities nor achieving desired coercive effects, often instead only further galvanizing an adversary's will to fight.<sup>99</sup>

---

<sup>97</sup> Schulze and Kerttunen, "Cyber Operations in Russia's War"; Lewis, "Cyber War and Ukraine."

<sup>98</sup> Schulze and Kerttunen recount how, in April 2022, when the Industroyer2 malware was found to be targeting industrial control systems in Ukraine's power grid, "incident responders were able to deactivate the...malware before its programmed timer was initiated," preventing it from having any effect, thus "undoing probably years of malware development." On the other hand, they point out, "conventional bombings were able to shut down more than forty per cent of Ukraine's power grid." If successful, the effort by the GRU's Sandworm (Unit 74455) could have deprived two million people of electricity. See Schulze and Kerttunen, "Cyber Operations in Russia's War"; Andy Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *Wired*, Apr. 12, 2022, <https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/>; and Lin, "Russian Cyber Operations."

<sup>99</sup> Schulze and Kerttunen, "Cyber Operations in Russia's War."

# Conclusion: Strategic Adaptation and the Wartime Cyber Debate

---

As the first major territorial war in Europe in many decades, pitting one of the world's leading military and cyber powers against its ostensibly weaker neighbor, the Russia-Ukraine war has been broadly considered as a testing ground for understanding the role of the cyber domain in modern full-scale warfare. But as we have seen, conclusions drawn so far by experts in the field have shown considerable variance. Of course, a certain amount of disagreement and uncertainty of this sort is inevitable at this early stage of analysis. After a year and a half of fighting, it is possible that we are still far from the end of this conflict. Not only are events still ongoing and ultimate strategic outcomes yet unclear, but the particularities of the cyber domain as a domain of often covert activity also create distinctive challenges for early analysis because of incomplete or asymmetric access to information within the analytical community. How can we make sense of this morass of disparate interpretations to draw maximally valid early lessons?

## Parsing the wartime cyber debate

Despite the discrepancies, some early assessments appear particularly noteworthy.

First, in spite of disagreements concerning their exact significance, available data and analytical assessments do indicate that Russia has mounted extensive cyber and information operations leading up to and during its war with Ukraine. Although these may not have had the maximalist, highly visible influence as expected in worst-case threat perceptions focused on the cyber domain's potential to create "bolt-from-the-blue" devastating "Cyber Pearl Harbor" types of events, it is likely too early to fully assess either the complete extent of these operations or their effects.

Second, it is also clear that Ukrainian defensive measures have played a critical role in blunting Russia's cyber offensive. These measures have included considerable learning and defensive hardening prior to the conflict as well as extensive public-private and international collaboration. These efforts demonstrate the potential power of cyber defense, also raising a significant theoretical prospect of an offense-defense balance that is more favorable to defenders. This prospect could also have meaningful implications for the cyber domain's future contributions to international stability or instability. But again, definitive conclusions here would be premature.

There also are still many questions.

What do the roles of Russian cyber and information operations in the war show about Russia's actual capabilities, strategy, and priorities in cyberspace and their merit as instruments of above-threshold warfare? Is it accurate to assess that Russia's numerous cyber and information operations have been of limited impact on achieving Russia's strategic war goals so far? If they have in fact been less consequential for the war effort than predicted by most in the Western strategic community, what explains this shortfall? Rival explanations emphasize Russian offensive blunders, Ukrainian defensive strength, inflated Western threat assessments, or more fundamental aspects of the domain itself. Some combination of these might all be true, but there are also potential risks in drawing the wrong lessons, which could lead to discounting threats prematurely in a way that opens Ukraine and the West to additional risks.

On the one hand, there is a real possibility that some pre-war assessments of the Russian cyber and informational threat were guilty of a degree of threat inflation, particularly along two dimensions. First, some assessments likely assumed too close a relationship between adversarial cyber *activity* and strategically relevant *effect*. Measuring effectiveness is difficult, particularly for activities such as subthreshold information campaigns or covert grey zone actions for which, in addition to attribution, any such measure also must account for adversary strategic intent. Insofar as these activities are believed to have strategic impact, this is often assumed to be iterative, "salami slicing," not instantaneous. A high degree of Western attention to Russian cyber-enabled influence activities since 2016, for example, has helped to create awareness of the problem, but the emphasis often has been more on accruing evidence of the activities themselves, rather than on (in this case often politically fraught) determinations of impact.

Second, some assessments of the Russian threat have also likely been premised on the assumption that what makes an actor quite capable in subthreshold cyber competition is the same as and will translate to above-threshold capability. This assumption deserves some unpacking: how useful are grey zone hybrid warfare tactics during an overt above-threshold war? Although covert operations and intelligence gathering will always have a place in warfighting, Russia's particular craft has often relied upon a mix of more and less precise activities, including a high volume of activities some of which have been facetiously described as "implausibly deniable"—sometimes leveraging lower skill, messier operations, proxy actors such as hacktivist groups or volunteers, and exploiting the evidentiary burden of legal or public attribution. Such techniques sometimes aim at populations made vulnerable to influence by prior beliefs, lack of awareness of Russian tactics, or limited attention to news or official state messaging channels. They benefit from the slow pace of research to catch up with and reveal numerous ongoing efforts and are most likely to be influential in contexts in which a small shift in public opinion can carry a significant difference in outcomes (such as in elections often decided by the thinnest of margins). It is less clear whether any of these conditions apply to a

wartime environment in which the would-be target population is galvanized around patriotic sentiment, is receiving regular public messaging updates from their government including warnings about attempted influence campaigns, where international open-source research communities and intelligence partners are paying particularly close attention to tracking and exposing Russian influence campaigns before they gain traction, and in which marginal changes in opinion might carry less weight relative to the overwhelming public support for the country's defensive efforts.

Too much focus on tactical and technical aptitude rather than force organization and strategic culture might explain some overly zealous predictions of fungibility between above- and below-threshold aptitude and impact. The Western strategic community might be guilty of some measure of mirror-imaging—assuming that a tactically skilled and technically capable adversary would use its capabilities in a similar fashion to us in the above-threshold environment, or that it would seek to execute the same worst-case scenarios that preoccupy our own threat perceptions.

On the other hand, and for related reasons, there are risks of discounting threats prematurely—creating greater potential future vulnerabilities. Just as subthreshold prowess might not prove as beneficial in an all-out conflict, there is also a risk of assuming that ineptitude demonstrated above threshold must necessarily translate to a similar weakness in below-threshold showing. Likewise, failure to have a strategic effect early in the conflict must not be considered necessarily predictive of continuing ineffectiveness. These risks could be particularly relevant in relation to Russia's ability to achieve a long-term effect on Ukraine's warfighting capability through external subthreshold cyber and information warfare. Ukraine's warfighting capacity is highly dependent upon an outside coalition of support—providing weapons, munitions, and other costly military aid. By targeting Ukraine's supporters, seeking to shift public sentiment about the war, sowing distrust, and undermining partnership cohesion, Russia could potentially leverage its greater strength in subthreshold activity to strategic advantage; it certainly is trying. Victory in the information war should not be declared prematurely. Appropriate efforts to address this threat could prove critical to the next stage of support for Ukraine's war effort.

There also is a danger in assuming away the possibilities of escalation and surprise too soon. Any move toward greater offense-defense parity in cyberspace is good news because of its likely ameliorative effects on first-strike instability pressures and risks of escalatory spiral. But, as we have argued elsewhere, the domain is also particularly prone to dynamics of mirror-imaging and of "concept misalignment" that can make misperceptions more likely.<sup>100</sup> The domain is also continuously evolving alongside the digital technological environment, meaning

---

<sup>100</sup> Kerr, "Concept Misalignment and Cyberspace Instability."

some traits bearing on stability, offense-defense balance, and the potential for surprise are unlikely to remain static.

## Information, adaptation, and learning

Drawing strategically and theoretically relevant conclusions based on observations of an ongoing conflict always poses grave challenges, including the early and incomplete nature of the evidence. A certain “fog of war” can certainly be said to apply to the strategic analytical community. The ongoing lack of consensus concerning the extent and role of cyber conflict in the current war, however, might be indicative of deeper challenges to strategically relevant wartime learning and adaptation in the cyber domain.

Experimentation, adaptation, and learning are critical in the maturation of any relatively new domain and further the development of its role in future strategy. Many of the initial findings from the Ukraine war demonstrate ongoing experimentation and adaptation by both sides in their uses of the cyber domain. This includes Russian attempts at joint cyber-and-conventional operations, even if not fully successful. It also includes their reuse of tailored versions of prior malware, including to prevent it from leaving Ukrainian networks (presumably to avoid inadvertent horizontal escalation). There are indications of maturing or changing cyber offensive and defensive organizational structures and novel uses of hacktivist networks and proxies. Ukraine’s defense has demonstrated dramatic shifts in the application of public-private, whole-of-government, and international collaboration. Western governments assisting in the defensive effort have likely honed and matured particular defensive strategies and operational approaches. A shift in favor of cyber defenders in this conflict, if real, would suggest major lessons for the future of cyber defense and defense collaboration going forward.

And yet, the dichotomous discourse highlights a broader challenge to learning lessons in the cyber domain: Researchers and analysts seeking to draw lessons are often coming at the problem from completely different angles, leading to some degree of incommensurability and miscommunication. They might be using different metrics to measure events or outcomes or be focused on different levels of analysis—directed more at tactical, operational, or strategic goals. They also frequently are not working from the same information. Enormous information asymmetries exist between analytical strategic expert and operational and technical communities. These asymmetries will be a challenge in tracking any ongoing conflict. But, more so than in most other domains or areas of strategic analysis, this gulf is made particularly daunting by the covert nature of much cyber domain activity, which raises daunting challenges for developing common modes of hypothesis testing and knowledge accumulation across the expert communities, potentially limiting opportunities for strategic-level analysis and learning in real time as part of the adaptation process.

Insofar as Russia has indeed underperformed in cyberspace during the current war, this likely relates, at least in part, to a failure to adequately bridge the divide between significant operational skill and technical talent, and strategic-level analysis and planning necessary to utilize these capabilities to the maximum coercive or warfighting effect. This failure is a good thing in the short term, for both Ukraine and the West. But it also can be considered a cautionary tale as this is a domain that constantly evolves and that will ultimately reward those actors most capable of bridging this divide, seamlessly allowing for agile strategic adaptation.

Adaptation and learning are vital in the successful adoption of new military capabilities, with innovative uses of emerging technologies or domains, frequently tested iteratively in the heat of battle. But strategic-level learning and adaptation often rely upon an interplay between this real-time tactical and operational experimentation and the theoretically-grounded observations of strategic analytical communities—sometimes far from the battlefield. The disconnects in wartime analysis across the cyber expert communities demonstrate both different modes of analysis and different levels of access to information. Although the former leads to potential mutual misunderstandings of strategically relevant measurements, the latter makes rapid public verification or falsification of strategic-level arguments dauntingly challenging, potentially limiting the effectiveness of real-time learning and adaptation during conflict.



# References

---

- Adamsky, Dmitry. "Cross-Domain Coercion: The Current Russian Art of Strategy." IFRI Security Studies Center. *Proliferation Papers* 54. Nov. 15, 2015.
- Akimenko, Valeriy, and Keir Giles. "Russia's Holistic Conceptual Framework for Cyber Activity." In *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, edited by Robert Chesney and Max Smeets, 173–200. Washington, DC: Georgetown University Press, 2023.
- Antoniuk, Daryna. "Ukraine's Cyber Chief on the Ever-Changing Digital War with Russia." The Record: Recorded Future News. May 21, 2023. <https://therecord.media/ukraine-ssscip-yurii-shchyhol-interview>.
- Asian News International. "US, UK Send Cyberwarfare Teams to Ukraine Amid Concerns Over Russia." *Business Standard*. Dec. 20, 2021. [https://www.business-standard.com/article/international/us-uk-send-cyberwarfare-teams-to-ukraine-amid-concerns-over-russia-121122100134\\_1.html](https://www.business-standard.com/article/international/us-uk-send-cyberwarfare-teams-to-ukraine-amid-concerns-over-russia-121122100134_1.html).
- Associated Press in London. "Ukraine Attacked by Cyberspies as Tensions Escalated in Recent Months." *Guardian*. Mar. 9, 2014. <https://www.theguardian.com/world/2014/mar/09/ukraine-attacked-cyberspies-tensions-computer>.
- Barnes, Julian E. "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections." *New York Times*. Feb. 26, 2019. <https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html>.
- Bateman, Jon, Nick Beecroft, and Gavin Wilde. "What the Russian Invasion Reveals About the Future of Cyber Warfare." In *Cyber Conflict in the Russia-Ukraine War Series*. Carnegie Endowment for International Peace. Dec. 19, 2022. <https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667>.
- Bateman, Jon. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." In *Cyber Conflict in the Russia-Ukraine War Series*. Carnegie Endowment for International Peace. Dec. 16, 2022. <https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657>.
- Beecroft, Nick. "Evaluating the International Support to Ukrainian Cyber Defense." In *Cyber Conflict in the Russia-Ukraine War Series*. Carnegie Endowment for International Peace. Nov. 3, 2022. <https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322>.
- BELZHD Live. "Порядок ввоза российского ядерного оружия в Беларусь" [Procedure for Importing Russian Nuclear Weapons into Belarus]. BELZHD Info. Community of Railway Workers of

- Belarus (SZhB). June 27, 2023, <https://belzhd.info/military-transportation/poryadok-vvoza-rossijskogo-yadernogo-oruzhiya-v-belarus/>.
- Benner, Katie, and Kate Conger. "US Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant." *New York Times*. Mar. 24, 2022. <https://www.nytimes.com/2022/03/24/us/politics/russians-cyberattacks-infrastructure-nuclear-plant.html>.
- Bronk, Christopher, Gabriel Collins, and Dan Wallach. "Cyber and Information Warfare in Ukraine: What Do We Know Seven Months In?" Baker Institute Issue Brief. Baker Institute for Public Policy. Rice University. Sept. 6, 2022. <https://doi.org/10.25613/69E1-WZ16>.
- Burgess, Matt. "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine." *Wired*. Mar. 23, 2022. <https://www.wired.com/story/viasat-internet-hack-ukraine-russia/?redirectURL=%2Fstory%2Fviasat-internet-hack-ukraine-russia%2F>.
- Burt, Tom. "Ongoing Russian Cyberattacks Targeting Ukraine." *Microsoft on the Issues (Microsoft blog)*. June 14, 2023. <https://blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyberattacks-ukraine-cadet-blizzard/>.
- Burt, Tom. "The Hybrid War in Ukraine." *Microsoft on the Issues (Microsoft blog)*. Apr. 27, 2022. <https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/>.
- Cattler, David, and Daniel Black. "The Myth of the Missing Cyberwar." *Foreign Affairs*. Apr. 6, 2022. <https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar>.
- Cerulus, Laurens. "How Ukraine Became a Test Bed for Cyberweaponry." *Politico*. Feb. 14, 2019. <https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/>.
- Conger, Kate, and David E. Sanger. "Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds." *New York Times*. Apr. 27, 2022. <https://www.nytimes.com/2022/04/27/us/politics/russia-cyberattacks-ukraine.html>.
- Connell, Michael, and Sarah Vogler. *Russia's Approach to Cyber Warfare*. CNA. Center for Naval Analyses. Mar. 2017.
- Cyber National Mission Force Public Affairs. "Before the Invasion: Hunt Forward Operations in Ukraine." US Cyber Command. Nov. 28, 2022. <https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/>.
- Cyber Peace Institute. "Attack Details." *Cyber Attacks in Times of Conflict*. Accessed Sept. 2023. <https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details>.
- Cyber Peace Institute. *Case Study: Viasat*. June 2022. <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat>.

- “Cyber-Attacks on Ukraine Are Conspicuous by Their Absence.” *Economist*. Mar. 1, 2022. <https://www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence>.
- Cybersecurity and Infrastructure Security Agency (CISA). “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.” Cybersecurity Advisory. May 9, 2022. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>.
- Davidoff, Victor. “Reading the Tea Leaves of Russia’s Pro-War ‘Z-Universe.’” *Moscow Times*. Oct. 14, 2022. <https://www.themoscowtimes.com/2022/10/13/reading-the-tea-leaves-of-russias-pro-war-z-universe-a79078>.
- Digital Forensic Research Lab (DFRLab). “Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression against Ukraine.” Atlantic Council. Feb. 22, 2023.
- Digital Forensic Research Lab (DFRLab). “Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine.” Atlantic Council. Feb. 22, 2023.
- Duffy, Kate. “A Top Pentagon Official Said SpaceX Starlink Rapidly Fought Off a Russian Jamming Attack in Ukraine.” *Business Insider*. Apr. 22, 2022. <https://www.businessinsider.com/spacex-starlink-pentagon-russian-jamming-attack-elon-musk-dave-tremper-2022-4>.
- Duffy, Kate. “Elon Musk Says Russia Has Stepped Up Efforts to Jam SpaceX’s Starlink in Ukraine.” *Business Insider*. May 11, 2022. <https://www.businessinsider.com/elon-musk-spacex-russia-ramps-up-efforts-jam-starlink-ukraine-2022-5>.
- “Estonia Hit by ‘Moscow Cyber War.’” BBC News. May 17, 2007. <http://news.bbc.co.uk/2/hi/europe/6665145.stm>.
- Fleming, Jeremy. “The Head of GCHQ Says Vladimir Putin Is Losing the Information War in Ukraine.” *Economist*. Aug. 18, 2022. <https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine>.
- Geers, Kenneth. “Computer Hacks in the Russia-Ukraine War.” Def Con 30. Aug. 11, 2022. <https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/>.
- Geers, Kenneth, Editor. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015. <https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/>.
- Giles, Keir. “Handbook of Russian Information Warfare.” Fellowship Monograph No. 9. NATO Defense College. Research Division. Nov. 2016.
- Giles, Keir. “The Next Phase of Russian Information Warfare.” NATO Strategic Communications Center of Excellence (COE). May 2016. <https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176>.

- Gonzalez, Gloria, Ben Lefebvre, and Eric Geller. "‘Jugular’ of the US Fuel Pipeline System Shuts Down After Cyberattack." *Politico*. May 8, 2021. <https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984>.
- Google Threat Analysis Group, Mandiant, and Google Trust & Safety, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," Google Report, Feb. 16, 2023.
- Greenberg, Andy. "Hackers Tied to Russia's GRU Targeted the US Grid for Years, Researchers Warn." *Wired*. Feb. 24, 2021. <https://www.wired.com/story/russia-gru-hackers-us-grid/>.
- Greenberg, Andy. "How an Entire Nation Became Russia's Test Lab for Cyberwar." *Wired*. June 20, 2017. <https://www.wired.com/story/russian-hackers-attack-ukraine/>.
- Greenberg, Andy. "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine." *Wired*. Apr. 12, 2022. <https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/>.
- Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*. Aug. 22, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- Greenberg, Andy. "Why the Belarus Railways Hack Marks a First for Ransomware." *Wired*. Jan. 25, 2022. <https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/>.
- Grossman, Taylor, Monica Kaminska, James Shires, and Max Smeets. "The Cyber Dimensions of the Russia-Ukraine War." Workshop Report. European Cyber Conflict Research Initiative (ECCRI). Apr. 20, 2023. <https://eccri.eu/events/the-cyber-dimensions-of-the-russia-ukraine-war/>.
- Healey, Jason, and Robert Jervis. "The Escalation Inversion and Other Oddities of Situational Cyber Stability." *Texas National Security Review* 3, no. 4. (2020): 30–53. <http://dx.doi.org/10.26153/tsw/10962>.
- Healey, Jason. "Not the Cyber Deterrence the United States Wants." *Council on Foreign Relations Blog*. June 11, 2018. <https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants>.
- Healey, Jason. "Preparing for Inevitable Cyber Surprise." *War on the Rocks*. Jan. 12, 2022. <https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/>.
- Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*. Jan. 6, 2011. <https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>.
- Huntley, Shane. "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape." *Google Updates from Threat Analysis Group*. Feb. 16, 2023. <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/>.
- Isaacson, Walter. "‘How Am I in This War?’ The Untold Story of Elon Musk’s Support for Ukraine." *Washington Post*. Sept. 7, 2023. <https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/>.

Jasper, Scott. *Russian Cyber Operations: Coding the Boundaries of Conflict*. Washington, DC: Georgetown University Press, 2020.

Jasper, Scott. "The Risk of Russian Cyber Retaliation for the United States Sending Rockets to Ukraine." *Council on Foreign Relations Blog*. June 15, 2022. <https://www.cfr.org/blog/risk-russian-cyber-retaliation-united-states-sending-rockets-ukraine>.

Kerr, Jaclyn A. "Concept Misalignment and Cyberspace Instability: Lessons from Cyber-Enabled Disinformation." In *Cyberspace and Instability*, edited by Robert Chesney, James Shires, and Max Smeets, 99–126. Edinburgh: Edinburgh University Press, 2023. <https://edinburghuniversitypress.com/book-cyberspace-and-instability.html>.

Kerr, Jaclyn A. "Runet's Critical Juncture: The Ukraine War and the Battle for the Soul of the Web." *SAIS Review of International Affairs* 42, no. 2 (2022): 63–84. <https://doi.org/10.1353/sais.2022.0011>.

Kostyuk, Nadiya, and Aaron Brantly. "War in the Borderland Through Cyberspace: Limits of Defending Ukraine Through Interstate Cooperation." *Contemporary Security Policy* 43, no. 3 (2022): 498–515. <https://doi.org/10.1080/13523260.2022.2093587>.

Kostyuk, Nadiya, and Erik Gartzke. "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine." *Texas National Security Review* 5, no. 3 (2022): 113–126. <http://dx.doi.org/10.26153/tsw/42073>.

Krebs, Chris. "The Cyber Warfare Predicted in Ukraine May Be Yet to Come: As Russia's Economy Deteriorates, the Red Lines Keeping Its Cyber Capabilities in Check May Evaporate." *Financial Times*. Mar. 20, 2022. <https://www.ft.com/content/2938a3cd-1825-4013-8219-4ee6342e20ca>.

Kristensen, Hans and Matt Korda. "Russian Nuclear Weapons Deployment Plans in Belarus: Is There Visual Confirmation?" Federation of American Scientists. June 30, 2023. <https://fas.org/publication/russian-nuclear-weapons-deployment-plans-in-belarus-is-there-visual-confirmation/>.

Lange-Ionatamišvili, Elina. *Analysis of Russia's Information Campaign Against Ukraine*. NATO Strategic Communications Centre of Excellence. 2015.

Latsinskaya, Maria, Alexander Bratersky, and Ignat Kalinin. "Rossiya vvela voyska v internet" [Russia Sent Troops to the Internet]. *Gazeta.Ru*. Feb. 22, 2017. [https://www.gazeta.ru/tech/2017/02/22\\_a\\_10539719.shtml](https://www.gazeta.ru/tech/2017/02/22_a_10539719.shtml).

"Lessons from Russia's Cyber-War in Ukraine." *Economist*. Nov. 30, 2022. <https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine>.

Lewis, James A. "Cyber War and Ukraine." Center for Strategic and International Studies (CSIS). June 16, 2022. <https://www.csis.org/analysis/cyber-war-and-ukraine>.

- Lilly, Bilyana. *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*. Annapolis, MD: Naval Institute Press, 2022.
- Lin, Herbert, and Jaclyn Kerr. "On Cyber-Enabled Information Warfare and Information Operations." In *Oxford Handbook of Cyber Security*, edited by Paul Cornish, 251–72. Oxford: Oxford University Press, 2022.
- Lin, Herbert. "Russian Cyber Operations in the Invasion of Ukraine." *Cyber Defense Review*. 2022.
- Lyngaas, Sean, and Phil Mattingly. "US Officials Prep Big Banks and Utilities for Potential Russian Cyberattacks as Ukraine Crisis Deepens." CNN Politics. Feb. 18, 2022. <https://www.cnn.com/2022/02/18/politics/treasury-banks-russia-cyber-meeting/index.html>.
- Markoff, John. "Before the Gunfire, Cyberattacks." *New York Times*. Aug. 12, 2008. <https://www.nytimes.com/2008/08/13/technology/13cyber.html>.
- Martin, Bradley, D. Sean Barnett, and Devin McCarthy. *Russian Logistics and Sustainment Failures in the Ukraine Conflict*. RAND. Jan. 1, 2023. [https://www.rand.org/pubs/research\\_reports/RRA2033-1.html](https://www.rand.org/pubs/research_reports/RRA2033-1.html).
- Maschmeyer, Lennart, and Nadiya Kostyuk. "There Is No Cyber 'Shock and Awe.'" *War on the Rocks*. Feb. 8, 2022. <https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/>.
- Maschmeyer, Lennart. "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security* 46, no. 2 (2021): 51–90. [https://doi.org/10.1162/isec\\_a\\_00418](https://doi.org/10.1162/isec_a_00418).
- Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2017.
- Melendez III, Marcos A., Michael E. O'Hanlon, and Jason Wolff. "America Can't Afford to Ignore the Logistics Triad." Brookings Institution. July 2023. <https://www.brookings.edu/articles/america-cant-afford-to-ignore-the-logistics-triad/>.
- Microsoft Digital Security Unit. "An Overview of Russia's Cyberattack Activity in Ukraine." Special Report: Ukraine. Apr. 27, 2022.
- Microsoft, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft Report, June 22, 2022, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>
- Miller, Maggie. "Biden's Options If Russia Hacks U.S. Infrastructure." *Politico*. Apr. 20, 2022. <https://www.politico.com/news/2022/04/20/biden-russia-hacks-00026384>.
- Miller, Maggie. "Russia Arrests Hacker in Colonial Pipeline Attack, US Says." *Politico*. Jan. 14, 2022. <https://www.politico.com/news/2022/01/14/russia-colonial-pipeline-arrest-527166>.

- Nair, Shalini. "Belarus Hackers Attack Train Systems to Disrupt Russian Troops." *Railway Technology*. Mar. 1, 2022. <https://www.railway-technology.com/news/belarus-hackers-attack-train-systems/>.
- National Cyber Security Centre. "New Analysis Highlights Strength of Ukraine's Defence Against 'Unprecedented' Russian Offensive." Apr. 20, 2023. <https://www.ncsc.gov.uk/news/new-analysis-eccri-highlights-ukraine-defence-against-russian-offensive>.
- Newman, Lily Hay. "Security News This Week: A Destabilizing Hack-and-Leak Operation Hits Moldova." *Wired*. Nov. 19, 2022. <https://www.wired.com/story/moldova-leaks-google-privacy-settlement-world-cup-apps/>.
- O'Neill, Patrick Howell. "Russia Hacked an American Satellite Company One Hour Before the Ukraine Invasion." *MIT Technology Review*. May 10, 2022. <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>.
- Pamment, James, Vladimir Sazonov, Francesca Granelli, Sean Aday, Māris Andžāns, Una Bērziņa-Čerenkova, John-Paul Gravelines, et al. "Hybrid Threats: 2007 Cyber Attacks on Estonia." NATO Strategic Communications Centre of Excellence, 2019. <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>.
- Pernik, Piret. "The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine." In *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, edited by Nicu Popescu and Stanislav Secieru. European Institute for Security Studies. Chaillot Paper No. 148. Oct. 2018.
- Raphelson, Samantha. "Report: Russian Hackers Had the Ability To Shut Down U.S. Power Plants." NPR. Mar. 16, 2018. <https://www.npr.org/2018/03/16/594371939/u-s-accuses-russia-of-cyberattacks-on-energy-infrastructure>.
- Recorded Future. "Russian Information Operations Aim to Divide the Western Coalition on Ukraine." *Cyber Threat Analysis: Russia*. Insikt Group. July 7, 2022. <https://www.recordedfuture.com/russian-information-operations-divide-western-coalition-ukraine>.
- Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5–32. <https://doi.org/10.1080/01402390.2011.608939>.
- Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus, and Giroux, 2020.
- Rollins, Sharon. "Defensive Cyber Warfare Lessons from Inside Ukraine." US Naval Institute. *Proceedings* 149, no. 6 (2023): 1,444. <https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine>.
- Rutenberg, Jim. "The Untold Story of 'Russiagate' and the Road to War in Ukraine." *New York Times Magazine*. Nov. 2, 2022. <https://www.nytimes.com/2022/11/02/magazine/russiagate-paul-manafort-ukraine-war.html>.

- Sakellariadis, John, and Maggie Miller. "Ukraine Gears Up for New Phase of Cyber War with Russia." *Politico*. Feb. 25, 2023. <https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429>.
- Sanger, David E. "Russian Hackers Appear to Shift Focus to US Power Grid." *New York Times*. July 27, 2018. <https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html>.
- Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown, 2018.
- Sanger, David E., and Julian E. Barnes. "US and Britain Help Ukraine Prepare for Potential Russian Cyberassault." *New York Times*. Dec. 20, 2021. <https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.html>.
- Sanger, David E., Julian E. Barnes, and Kate Conger. "As Tanks Rolled into Ukraine, So Did Malware. Then Microsoft Entered the War." *New York Times*. Feb. 28, 2022. <https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html>.
- Schneier, Bruce. "An Example of Deterrence in Cyberspace." *Schneier on Security*. June 7, 2018. [https://www.schneier.com/blog/archives/2018/06/an\\_example\\_of\\_d.html](https://www.schneier.com/blog/archives/2018/06/an_example_of_d.html).
- Schulze, Matthias, and Mika Kerttunen. "Cyber Operations in Russia's War Against Ukraine." Stiftung Wissenschaft und Politik (SWP). German Institute for International and Security Affairs. SWP Comment No. 23. Apr. 17, 2023. doi:10.18449/2023C23.
- Seldin, Jeff. "US Bracing for Bolder, More Brazen Russian Cyberattacks." *VOA News*. Mar. 7, 2023. <https://www.voanews.com/a/us-bracing-for-bolder-more-brazen-russian-cyberattacks/6992938.html>.
- Sganga, Nicole. "'It's Coming': President Biden Warns of 'Evolving' Russian Cyber Threat to U.S." *CBS News*. Mar. 21, 2022. <https://www.cbsnews.com/news/russia-cyber-attack-threat-biden-warning/>.
- Sharkov, Damien. "Russia Announces 'Information Operations' Troops With 'Counter-Propaganda' Remit." *Newsweek*. Feb. 22, 2017. <https://www.newsweek.com/russia-announces-information-operations-troops-counter-propaganda-559656>.
- Shchyhol, Yurii. "Vladimir Putin's Ukraine Invasion Is the World's First Full-Scale Cyberwar." *Atlantic Council*. June 15, 2022. <https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-ukraine-invasion-is-the-worlds-first-full-scale-cyberwar/>.
- Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (2016–17): 72–109. <https://www.jstor.org/stable/26777791>.



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

Snegovaya, Maria. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare." Institute for the Study of War (ISW). Russia Report I. Sept. 2015.

Soldatov, Andrei, and Irina Borogan. "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities." The Center for European Policy Analysis (CEPA) Reports. Sept. 8, 2022. <https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/>.

Sun, Mengqi, and Richard Vanderford. "U.S. Banks Are Prepared for Russia Sanctions, but Concerns Grow About Potential Hacks." *Wall Street Journal*. Feb. 24, 2022. <https://www.wsj.com/articles/u-s-banks-are-prepared-for-russia-sanctions-but-concerns-grow-about-potential-hacks-11645743246>.

The Associated Press. "Bluffing or Not, Putin's Declared Deployment of Nuclear Weapons to Belarus Raises Tensions." AP News. July 27, 2023. <https://apnews.com/article/russia-ukraine-war-belarus-putin-nuclear-3bc2aefef4ee6b4478c81ae76bebdd4e>.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *Guardian*. May 16, 2007. <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.

Van Sant, Shannon. "Kyiv Argues Russian Cyberattacks Could Be War Crimes." *Politico*. Jan. 9, 2023. <https://www.politico.eu/article/victor-zhora-ukraine-russia-cyberattack-infrastructure-war-crime/>.

Vanberghen, Cristina. "Ukraine Marks a Turning Point for Cyberwarfare." *Politico*. Dec. 28, 2022. <https://www.politico.eu/article/russia-ukraine-cyber-invasion-warfare-kremlin-nato/>.

Vasques, Christian, and Elias Groll. "Satellite Hack on Eve of Ukraine War Was a Coordinated, Multi-Pronged Assault." *Cyberscoop*. Aug. 10, 2023. <https://cyberscoop.com/viasat-ka-sat-hack-black-hat/>.

Vičić, Jelena, and Rupal N. Mehta. "Why Russian Cyber Dogs Have Mostly Failed to Bark." *War on the Rocks*. Mar. 14, 2022. <https://warontherocks.com/2022/03/why-cyber-dogs-have-mostly-failed-to-bark/>.

Volz, Dustin, and Robert McMillan. "In Ukraine, a 'Full-Scale Cyberwar' Emerges." *Wall Street Journal*. Apr. 12, 2022. <https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203>.

Walker, Owen, and Imani Moise. "Banks on Alert for Russian Reprisal Cyber Attacks on Swift." *Financial Times*. Mar. 15, 2022. <https://www.ft.com/content/a2bdba3b-f1dd-4c9f-a0de-9ffff6e744e4>.

- Watts, Clint. "Is Russia Regrouping for Renewed Cyberwar?" *Microsoft on the Issues (Microsoft blog)*. Mar. 15, 2023. <https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center/>.
- White, Sarah P. "Understanding Cyberwarfare: Lessons from the Russia-Georgia War." Modern War Institute. Mar. 20, 2018. <https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/>.
- "Why Russia's Cyber-Attacks Have Fallen Flat." *Economist*. Dec. 1, 2022. <https://www.economist.com/leaders/2022/12/01/why-russias-cyber-attacks-have-fallen-flat>.
- Wilde, Gavin, and Justin Sherman. "Targeting Ukraine Through Washington." Atlantic Council Issue Brief. Mar. 2022. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/targeting-ukraine-through-washington/>.
- Wilde, Gavin. "Cyber Operations in Ukraine: Russia's Unmet Expectations." *Cyber Conflict in the Russia-Ukraine War Series*. Carnegie Endowment for International Peace. Dec. 12, 2022. <https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607>.
- Work, JD, and Richard Harknett. "Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges." Atlantic Council Issue Brief. July 22, 2020. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/>.
- Zetter, Kim. "The Untold Story of the Boldest Supply-Chain Hack Ever." *Wired*. May 2, 2023. <https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/>.

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

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

Any copyright in this work is subject to the Government's Unlimited Rights license as defined in DFARS 252.227-7013 and/or DFARS 252.227-7014. The reproduction of this work for commercial purposes is strictly prohibited. Nongovernmental users may copy and distribute this document noncommercially, in any medium, provided that the copyright notice is reproduced in all copies. Nongovernmental users may not use technical measures to obstruct or control the reading or further copying of the copies they make or distribute. Nongovernmental users may not accept compensation of any manner in exchange for copies.

All other rights reserved. The provision of this data and/or source code is without warranties or guarantees to the Recipient Party by the Supplying Party with respect to the intended use of the supplied information. Nor shall the Supplying Party be liable to the Recipient Party for any errors or omissions in the supplied information.

This report may contain hyperlinks to websites and servers maintained by third parties. CNA does not control, evaluate, endorse, or guarantee content found in those sites. We do not assume any responsibility or liability for the actions, products, services, and content of those sites or the parties that operate them.



Dedicated to the Safety and Security of the Nation

CNA is a not-for-profit research organization that serves the public interest by providing in-depth analysis and result-oriented solutions to help government leaders choose the best course of action in setting policy and managing operations.

IOP-2023-U-037223-Final

3003 Washington Boulevard, Arlington, VA 22201

[www.cna.org](http://www.cna.org) 703-824-2000