

ON FUTURE WAR

July 2023

Cyber Operations during the Russo-Ukrainian War

From Strange Patterns to Alternative Futures

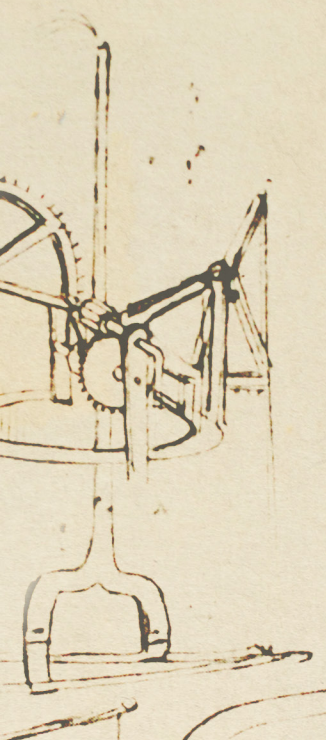
By Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias

In the Future . . .

- **Cyber operations will play a supporting rather than decisive role in major theater wars.** Great powers will continue to invest in cyber capabilities but see diminishing returns on these investments outside of intelligence and deception efforts once major conflict breaks out.
- **War will still be a continuation of politics by other means and rely on the more tangible effects of violence than on the elusive effects of compromising information networks.** During the transition to warfighting, military commanders will prefer the certainty of lethal precision strikes against high-value targets to the uncertainty of generating effects in cyberspace.
- **The merits of cyber operations continue to be their utility as a tool of political warfare because they facilitate an engagement short of war that leverages covert action, propaganda, and surveillance but in a manner that poses a fundamental threat to human liberties.** Cyber operations will remain a limited tool of coercion. Due to their uncertain effects, military leaders will initiate fewer critical cyber operations against command and control and military targets than currently anticipated. They will also face fewer restrictions on waging information warfare to mobilize and shape discontent.

Introduction

How central are cyber operations to combined arms campaigns in the twenty-first century? Between the spring of 2021 and winter of 2022, Russian military forces began to mass combat troops along Ukraine's eastern border. On February 24, 2022, Russia invaded Ukraine. It marked the fourth time Russia used military force against a neighbor since the end of the Cold War and the seventh time Russia used cyber operations as part of a larger campaign or independently as an instrument of coercion against a neighboring state.¹



Pundits and academics alike came out with grand predictions about a coming cyber war.² Researchers from the North Atlantic Treaty Organization (NATO) even argued during the war that “Russian cyberattacks on government and military command and control centers, logistics, emergency services . . . were entirely consistent with a so-called thunder run strategy intended to stoke chaos, confusion, and uncertainty, and ultimately avoid a costly and protracted war in Ukraine.”³

This edition of the *On Future War* series uses an empirical analysis of attributed Russian cyber operations in Ukraine to extrapolate future scenarios for the use of cyber operations in major theater wars below the nuclear threshold. The best predictions about an uncertain future come from analysis of past attack patterns and trends as well as seminal cases—such as Ukraine—that are almost certain to change the character of war. Reference the *Statistical Appendix* for more information.

Into the war’s second year, Russia remains locked in a protracted conventional conflict that, in addition to pitched battles and missile strikes, has seen sabotage, forced displacement and kidnapping of children, systematic rape and torture, and threats to use nuclear weapons. Yet, Russia has not launched an all-out, costly cyberwar against Ukraine or its backers in the West. The so-called “thunder run” never materialized.⁴ Rather, a mix of Ukrainian determination, the characteristics of the cyber domain, and a Russian preference for waging a global campaign focused more on misinformation and undermining support for Kyiv appear to have taken its place.

This installment of *On Future War* analyzes Russian cyber operations linked to the war in Ukraine. This study uses the publicly attributed record of Russian cyber operations in Ukraine to extrapolate insights about the character of cyber operations as instruments of warfighting and coercion in the twenty-first century. The empirical evidence demonstrates that while there has been an uptick in cyberattacks during the conflict, these attacks did not demonstrate an increase in severity, a shift in targets, or a shift in methods. Despite proclamations of doom, gloom, and a revolution in warfare, Russia behaved in a manner contrary to most popular expectations during the conflict. While cyber-enabled targeting at the tactical level is almost certain to occur alongside signals intelligence—a practice first documented in Ukraine in 2016—the prevailing trends suggest cyber operations have yet to make a material impact on the battlefield.⁵ Where Russian cyber operations have made a difference is in their support to information operations and propaganda in the Global South, where Moscow has successfully spread disinformation to undermine support to Ukraine. Similar to earlier academic treatments that find cyber operations play a key role in shaping intelligence, deception, and political warfare, the Ukrainian case illustrates that the digital domain plays a shaping rather than decisive role even during extensive and existential combat.⁶

In addition to casting doubt on the cyber thunder run, the empirical record, especially when compared to previous Russian cyber operations, offers a baseline prediction about the future and how states will integrate cyber operations into a spectrum of conflict ranging from crises to major wars.⁷ While the system could evolve and cyber operations might prove to be decisive instruments of war in the future, the record to date suggests alternatives for how this technology will be leveraged on the battlefield. Specifically, integrating the empirical record of cyber operations in Ukraine alongside well-established findings from the quantitative study of war suggests three scenarios.





1. **Cyber Stalemate:** Russia struggles to integrate cyber and conventional effects on the battlefield and beyond due to the resilience of cyber defense as well as the power of public-private partnerships.
2. **War Comes Home:** Russia regroupes and launches a wave of cyberattacks against critical U.S. infrastructure.
3. **Digital Lies:** Russian cyber-enabled influence operations and computational propaganda degrade support for the United States and the war in Ukraine.

Looking across these scenarios suggests key policy options—each consistent with active campaigning and integrated deterrence—the Biden administration could take over the next two years to shape what will likely be a long-term competition with Russia that extends deeper into the twenty-first century. Over time it has become clear that resilience and a focus on defensive operations can forestall the potential impact of offensive cyber operations. Defense in cyberspace requires expanding public-private partnerships and collaboration alongside pooled data to identify attack patterns and trends. Last, the United States and its partners will need to develop better ways and means for countering how malign actors such as Russia use cyberspace to distort global public opinion. For every failed network intrusion, there are thousands of successful social media posts skewing how the world looks at the war in Ukraine.

Making Sense of Cyber Operations

U.S. joint doctrine defines cyberspace operations as the “employment of cyberspace capabilities where the primary purpose is to achieve objectives in and through cyberspace.”⁸ Cyberspace is further defined as an “interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”⁹

From a military perspective, groups seek to defend their networks while infiltrating other networks through the different layers of cyberspace (i.e., physical, logical, and persona). As a result, network access is turned into an intelligence advantage or means of delivering effects, creating unique “use-lose” trade-offs in cyber operations.¹⁰ Disrupting or degrading adversary networks risks losing intelligence access. In addition, the dual effort to gain and exploit access does not take place on a battlefield but often in commercial systems and networks, creating unique dilemmas as patches and updates can dislodge or distort cyber payloads. Last, many cyber operations rely on similar tactics, techniques, and procedures, meaning that compromising one operation can result in a cascading effect compromising other operations.

While cyber operations, by design, tend to be concealed, with cyber operators often masking their intrusions and identities by routing payloads through third-party servers, it is possible to analyze how state and non-state actors use cyberspace to advance their interests. Academics, governments, and threat intelligence firms have been cataloging cyber operations for over 20 years. This treatment follows academic research and employs a systematic coding standard as opposed to simple lists that avoid peer review and replication.¹¹ The underlying assumption about external validity is that documented cyber incidents and associated campaigns are representative of the larger universe of cyber incidents that are unseen or unreported.¹²

For many, cyber operations are a method to enable a decisive advantage, creating an easy path to victory. As Josh Rovner, associate professor at the School of International Service at American University, notes, “For policymakers and planners, cyberspace operations suggest a low-cost route to quick and decisive victories.”¹³ This idea is developed most clearly in Jan Kallberg’s theory of

Figure 1: Common Cyber Myths

Cyber operations are decisive.



Cyber operations are offense dominant.



Cyber operations set the conditions for political collapse.



Source: CSIS.

decisive cyber operations.¹⁴ Kallberg, a former research scientist with the Army Cyber Institute at West Point, argues that “the decisive cyber outcome is either reached by removing military capacity through cyber attacks or destabilization of the targeted society.”¹⁵ The idea is to trigger a “dormant entropy embedded in a nation possessing weak institutions.”¹⁶

Many visions of decisive cyber victory emerge from the idea that cyber warfare represents a revolution in war and military affairs.¹⁷ Amit Sharma, formerly of India’s Ministry of Defence, note, “Cyber warfare . . . is a warfare which is capable of compelling the enemy to your will by inducing strategic paralysis to achieve desired ends and this seizing of the enemy is done almost without any application of physical force.”¹⁸

Greg Rattray, former director of cybersecurity for the White House, offered that “successful integration of information systems in a sophisticated conventional force capability proved decisive

during the spectacular U.S. military successes in the Gulf War.”¹⁹ But he also further cautioned that challenges, including expertise for targeted attacks, the difficulty in assessing the political consequences for information disruption, and defensive coordination challenges, would hamper the ability of information warfare to be effective in generating effects.²⁰

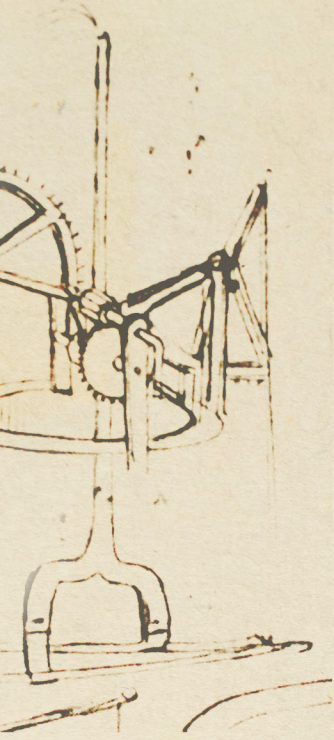
Applied to Ukraine, the vision of decisive cyber victory imagined Russian network intrusions extending beyond battlefield objectives to undermine confidence in Kyiv. Kallberg’s original theory focused on weak states where “cyber targeting can induce a sense of lack of control with citizens blaming the state for failing to safe-guard the societal structure.”²¹ In many ways, this was the vision Russia had of Ukraine, seeing a quick war as sufficient to destabilize the government and lead to a general collapse, leaving Moscow in control of the country. Keith Alexander, former director of the National Security Agency (NSA) and U.S. Cyber Command, noted “a cyber attack—which is relatively easy and comparatively cheap—is likely to top that list. As Russia showed during the 2008 Georgia conflict, hacking government systems as well as financial and energy sectors can cause chaos.”²²

NATO analysts David Cattler and Daniel Black point to cyber operations as “Russia’s biggest military success to date in the war in Ukraine.”²³ Keir Giles, a senior consulting fellow at Chatham House, goes so far as to argue that conventional operations would not even be needed:

It is hard to see how rolling tanks across the border would serve Russia’s aims when far cheaper and more controllable options exist for inflicting damage on Ukraine. . . . Stand-off strikes using missiles, or potentially a destructive cyber onslaught, could target military command and control systems or civilian critical infrastructure and pressure Kyiv into concessions and its friends aboard into meeting Russia’s demands.²⁴

This logic is reminiscent of airpower theorists in the interwar period who believed bombers would destroy cities, forcing citizens to pressure their governments into surrendering.²⁵

Extending the idea to Ukraine’s foreign backers, Jason Healey, a senior research scholar at Columbia University, notes that another SolarWinds-style attack on the United States would be a “psychological shock to the public and to decision-makers” and “might successfully coerce the United States into backing down.”²⁶ Fear that Russia would escalate and expand the conflict to the United States through cyber means motivated the desire for many to remain neutral, or to at least have “shields up.”²⁷



Scholars working at the intersection of international security and disruptive technology generally reject the idea of a decisive victory in cyberspace.²⁸ Academics such as Nadiya Kostyuk and Erik Gartzke note that Russian cyber operations “have neither supplanted nor significantly supplemented conventional combat activities.”²⁹ Others state, “We are less convinced of effective Russian or Ukrainian battlefield cyber action.”³⁰ Earlier researchers noted that “despite increasingly sophisticated operations, between 2000 and 2016 cyberspace was a domain defined by political warfare and covert signaling to control escalation more than it was an arena of decisive action.”³¹ Instead, cyber operations generally represent covert or deception operations seeking to coerce or signal to the adversary.³² Often linked to intelligence, cyber operations act more like complementary activities in war than singularly decisive instruments.³³ Like combined arms, cyber operations work best when integrated with other effects to create multiple dilemmas for an adversary. This logic implies that Russian cyber operations in Ukraine were likely restrained by the character of cyberspace and its strategic logic.³⁴

There is also the possibility that cyber operations are more defensive rather than offensive. The majority of code, computer equipment, and network infrastructure in the world is owned and operated by private companies. These companies spend billions of dollars monitoring their networks. A mix of nonprofits and academics constantly search for bugs and update companies about deficiencies. This unique feature of cyber competition means that even the best laid plans are often undone by the ecosystem of firms and citizens seeking to secure cyberspace. In addition, the human capital and costs required to develop high-end cyber effects can constrain their use.³⁵ Work by the U.S. Cyberspace Solarium Commission highlighted this dynamic and encouraged building layers in national cyber strategy to deny easy access and change the costs adversaries expect to pay to attack U.S. interests.³⁶

Russian Cyber Operations

Historical Cases

Looking at the history of Russian cyber operations, the Kremlin employs cyber means to engage in long-term competition with rivals.³⁷ Before 2014, Moscow’s campaigns tended to focus on political warfare and espionage. Operations in Estonia and Georgia were the most prominent. Massive denial-of-service operations sought to punish Estonia in 2007 after the country moved the Russian monument known as the Bronze Soldier.³⁸ During the Russo-Georgian conflict of 2008, Russia leveraged cyberattacks to enable information operations (IO) against Georgia.³⁹ Russian’s IO operations aimed “to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting [their] own.”⁴⁰

In a harbinger of its military campaign to destroy Ukrainian critical infrastructure, Moscow also used cyber operations to target Kyiv’s power supply. Following the illegal annexation of Crimea in 2014, advanced persistent threat (APT) groups such as Sandworm were implicated in the 2015 BlackEnergy campaign targeting Ukrainian power generation and distribution.⁴¹ While the attacks captured headlines, they produced limited effects.⁴² In 2017, Russian-linked groups launched the NotPetya campaign, which produced effects that spilled over from the intended targets, Ukrainian companies, to affect global logistics.⁴³

Russia has also used cyber operations as a form of political warfare, using a mix of propaganda to polarize societies and influence political elections. Of note, these efforts included parallel disruption campaigns seeking to deface websites and portray supporters for Ukraine as Nazis.⁴⁴ This campaign was followed by the even more audacious attempt to undermine confidence in



U.S. democracy through the 2016 operations targeting the presidential election, where the effects are still debated.⁴⁵ In 2018, U.S. Cyber Command used Russia's past behavior as well as other indicators and warnings that Moscow was about to repeat its efforts as justification for launching a preemptive operation against the Internet Research Agency, a Russian propaganda and influence operation firm, designed to forestall attacks during the midterm elections.⁴⁶

More recently, Russian operations have combined a mix of sophisticated espionage and criminal malware campaigns. For most of 2020, the Russian hacking group APT29, or Cozy Bear, exploited a supply chain vulnerability in the SolarWinds Orion program to exfiltrate data and digital tools from an extensive list of targets.⁴⁷ The operation raised alarm bells since neither the NSA nor major firms such as Microsoft detected the intrusion and because it likely involved a combination of human intelligence and cyber operations to insert malicious code deep into servers. In 2021, criminal actors known as DarkSide, likely linked to the Russian state, were successful in deploying ransomware against Colonial Pipeline, the system that moves much of the fuel used across the United States' East Coast.⁴⁸

Empirical Analysis

These high-profile examples parallel the prevailing empirical pattern of Russian cyber operations between 2000 and 2020. The latest version of the Dyadic Cyber Incident and Campaign Data (DCID 2.0) extends the timeline of the dataset and adds new variables, including ransomware and information operations.⁴⁹ The dataset codes cyber incidents indicative of larger campaigns and establishes a typology for strategic objectives, including disruption (causing low-cost, low-pain incidents), short-term espionage (gaining access for immediate effect), long-term espionage (leveraging information for future operations), and degrade (pursuing physical destruction and impairment). Severity is measured on an interval scale between 0 and 10. Where (0) is no cyber activity (1) and begins tracking the impact of cyber operations of passive operations to (4) widespread government, economic, military, or critical private sector network intrusion, multiple networks to (5) single/multiple critical network infiltration and physical attempted destruction, with (10) a potential outcome of massive deaths.⁵⁰ This coding methodology follows practices established in political science to study crises, disputes, and conflicts since the 1960s.⁵¹

Between 2000 and 2020, there were 30 recorded dyadic cyber incidents indicative of larger campaigns between Russia and Ukraine. Russia was frequently the initiator but rarely the target. Of the 30 recorded cyber events between Russia and Ukraine, 28 (or 93 percent) were initiated by Russia. Over this period, the majority of Moscow's targets (57 percent) were private, non-state actors. Only 11 percent of documented Russian cyber operations targeted government military targets. This targeting profile suggests that Moscow struggles to compromise more defended Ukrainian networks. While crucial cases such as SolarWinds suggest the possibility of more, yet-to-be-detected instances of cyber campaigns supported by human intelligence operations that are hard to detect, available data suggests that cyber defenses are holding in Ukraine.

Many of Russia's past cyber incidents and campaigns targeting Ukraine were launched for disruption or espionage purposes rather than to degrade critical government networks. Only 29 percent of the documented cyber incidents indicative of larger campaigns were degradations. The majority of Russian cyber operations were characterized by phishing attempts, distributed denial-of-service campaigns, propaganda or vandalism efforts, and single network intrusions—all of which tend to have a limited impact.

Altogether, none of the 28 recorded cyber incidents indicative of larger campaigns were so severe



that they resulted in lasting physical damage. On a scale from 0 to 10, with “0” representing no cyber activity and “10” representing massive death as a direct result of a cyber incident, Russia’s attacks targeting Ukraine never surpassed a “5”—single or multiple critical network infiltrations and attempted physical destruction. Furthermore, none of Russia’s past cyber operations resulted in a concessionary change in the behavior of Ukraine. Moscow appears to view using cyber operations more as a means of harassing Ukraine and supporting information operations than as a war-winning weapon indicative of the thunder run strategy.

This pattern of behavior is largely consistent with Russia’s interactions with its other rivals. According to the DCID 2.0 dataset, of the 113 total cyber incidents and larger campaigns documented that Russia initiated against its rivals between 2000 and 2020, only one (0.088 percent) resulted in a tangible political concession. Cyber operations remain a weak coercive instrument for Moscow despite their frequent use.

Analysis of Russian Cyber Operations in 2022

Turning from the DCID 2.0 dataset to the first year of the war in Ukraine, the CSIS research team identified 47 publicly attributed cyber incidents indicative of a campaign initiated by Russia between November 29, 2021, and May 9, 2022.⁵² This data is culled directly from Ukrainian government sources and Microsoft reports, avoiding the biases that might be introduced by many contemporary news accounts. Because of the covert nature of cyber operations, it is likely only a small but representative sample of the larger population intrusions.

If the character of cyber operations aligns more with intelligence and shaping activities such as deception, one would expect to see this tendency in the early stages of the war in Ukraine. In other words, observations from datasets such as the DCID 2.0 should show, even if they are only a small sample of the larger population, that cyber operations increased in frequency but not severity in the initial stages of the 2022 conflict compared to prewar statistics. Since it is difficult to know exactly when a cyber campaign begins, the data should show a lag resulting in spikes around the beginning of major hostilities.

This condition is exactly what emerged from reviewing the pattern of cyber intrusions captured by the DCID 2.0. There was a 75 percent increase in documented cyber intrusions—but a decline in the average severity of the attack. The severity level for the average fell after the full-scale invasion, indicating that although low-level disruption and espionage have continued, there has been a significant drop in degradation-type operations coming from Russia. The results are statistically significant and reported in the Statistical Appendix. What is unknown is whether this decline is a function of deliberate targeting or the resiliency of Ukrainian cyber defenses, issues addressed later in this study.

Contrary to speculation that Russian targets would shift to focus on supporting military operations, an analysis of the DCID 2.0 shows no statistically significant change in targeting or the overall campaign type. There was no statistically significant difference in targeting before and after the invasion (see Statistical Appendix). This finding suggests that the utility of cyber operations rests in setting conditions and intelligence more than in direct application during large-scale

Cyber operations remain a weak coercive instrument for Moscow despite their frequent use.

combat operations. While cyber-enabled targeting supports combat, the data shows that larger cyber campaigns do not radically shift during wartime. What the findings cannot determine is whether or not this observation is a function of the character of

There was no statistically significant difference in targeting before and after the invasion . . . the utility of cyber operations rests in setting conditions and intelligence more than in direct application during large-scale combat operations.

have remained disruptive shaping activities and cyber espionage campaigns. During the first few months of its 2022 invasion of Ukraine, disruption incidents comprised 57.4 percent of the total incidents, followed by espionage (21.3 percent).

Reliance on disruptive operations stands in contrast to Russia's prewar behavior, which accentuated espionage. That said, for both the prewar sample and the 2022 war sample, degradative cyber operations were never the majority. Just as Russia's past cyber operations failed to result in any Ukrainian concessions, no concessions were made by Ukraine during the timeframe of this analysis.

During war, a state might alter its cyber targeting. Yet this analysis of Ukrainian cyber events fails to confirm this hypothesis. Looking at the targets of Russian cyber aggression in the 47 total incidents, most (59.6 percent) targeted private non-state actors, followed by attacks targeting state and local government actors (31.9 percent). Just four (or 8.5 percent) targeted government military actors. This target-type breakdown closely corresponds to Russia's targets between 2000 and 2020: 57 percent of the targets were private non-state actors, 32 percent were government nonmilitary actors, and 11 percent were government military actors. It is counterintuitive that military actors have not been targeted more frequently during the war.

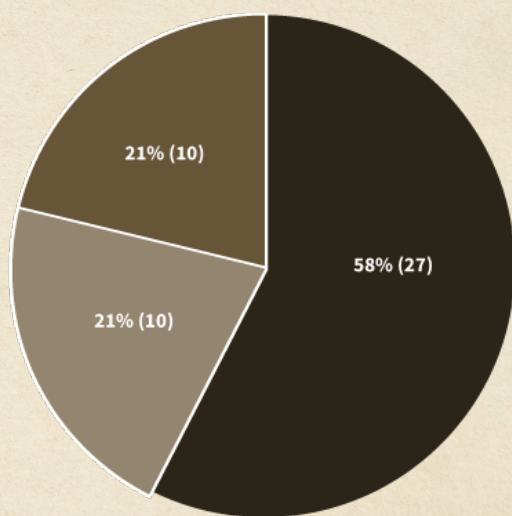
These results cast doubt on the extent to which Russia has successfully integrated its conventional military operations with cyber effects. Coordination with conventional forces became an important talking point, with a large segment of the news media following some analysts in making the claim that there was significant coordination between cyber operations and conventional military forces.⁵³

This analysis fails to substantiate these claims. Russian military operations appear to struggle

cyberspace or the result of case-specific factors such as the resiliency of Ukraine's cyber defense.

Looking at the style of Russian attacks, the research team found that Russia's cyber activity during the war has been more disruptive than degrading, consistent with its past behavior. As seen in Figure 2, when one looks at these cyber operations by type, Moscow's preferred cyber objectives

Figure 2: Russian Cyber Objectives Targeting Ukraine, 2022



■ Disruption ■ Espionage ■ Degradation

Source: CSIS.

These results cast doubt on the extent to which Russia has successfully integrated its conventional military operations with cyber effects.

with integrating combined effects, especially across domains.

This seeming lack of coordination between cyber and conventional attacks is something likewise acknowledged by James Lewis, senior vice president at CSIS. To pull off a

successful, coordinated attack requires both planning and intelligence support, and either because it chose not to do this or it was incapable of doing so, Russia's cyber efforts have had a limited effect on Russia's military efforts in Ukraine. This leads Lewis to candidly state, "Cyberattacks are overrated. While invaluable for espionage and crime, they are far from decisive in armed conflict."⁵⁴

These results cast doubt on the extent to which Russia has successfully integrated its conventional military operations with cyber effects.

Making Sense of the Findings

There was a dramatic increase in cyber operations during the initial stage of the war. Yet paradoxically, there was no corresponding change in severity or style, nor shifts in Russia's target preferences. While the rate of cyber conflict increased during the war, the rate of concessions or even severe cyber operations did not. This empirical baseline, albeit based on aggregating unclassified data, demands an explanation.

The analysis offered above provides an insight into what is happening but not necessarily a clear explanation for why it is happening. Below, this study considers three different causal explanations. The first—which follows the logic of the data collected and assessed above, as well as minority reports—offers an explanation for why Russian cyber efforts have been ineffective.⁵⁵ The second considers the opposite: why the world could still witness widespread cyber campaigns in Ukraine and beyond. The third considers an alternative logic of cyberspace focused on misinformation, disinformation, and malinformation, as well as larger propaganda campaigns.

1. "The Defense Is Dominant"



There is the possibility that a combination of private sector innovation, state coordination, and emerging doctrine have made the cyber domain defense dominant. While SpaceX and Starlink captured headlines from Ukraine, multiple firms raced to help the country retain the ability to access cyberspace.⁵⁶ Microsoft reported that a mix of "cyber threat intelligence and end-point protection . . . helped Ukraine withstand a high percentage of destructive Russian cyberattacks."⁵⁷ Even where Russia coordinated wiper attacks and cruise missile strikes against data centers, Ukraine was able to "disburse its digital infrastructure into the public cloud" and survive the onslaught.⁵⁸ In November 2022, Ukrainian deputy prime minister and minister for digital transformation, Mykhailo Fedorov, praised Amazon Web Services (AWS) for their role in helping Ukraine maintain continuity of government during the war.⁵⁹ During the opening stages of the conflict, AWS sent in suitcase-sized computer drives to help Ukraine back up critical data.⁶⁰ Cybersecurity firm Cloudflare extended its Project Galileo services—a full suite of protection for organizations in the arts, human rights, civil society, journalism, and democracy promotion—to key organizations across Ukraine.⁶¹ This effort paralleled Google's Project Shield, which similarly seeks to help at-risk organizations defend against cyber intrusions.⁶² In all, the character of cyberspace, which relies on business networks and the public sector, means that a web of private actors have been enmeshed with the defense of Ukraine.⁶³



Beyond new technology that increases the power of the defense, the last seven years have seen an unreported push to coordinate cybersecurity policies across states and involve the private sector.⁶⁴ The architects of Ukrainian cyber strategy participated in multiple U.S. Department of State initiatives, including meeting with the research director for the U.S. Cyberspace Solarium Commission a year before the conflict began. Multiple federal agencies have programs supporting Ukraine's networks and digital infrastructure that predate the war, including cybersecurity reform initiatives from the U.S. Agency for International Development and initiatives in the Department of Homeland Security and Department of Justice for sharing threat information.⁶⁵ These efforts paralleled similar EU initiatives.⁶⁶

The concept of what constitutes defensive mechanisms in cyberspace has also evolved over the last 10 years. Early cyber strategies released by the U.S. Department of Defense tended to be criticized as being too defensive.⁶⁷ Following the lead of the 2018 National Defense Strategy and parallel initiatives across the Department of Defense, U.S. Cyber Command also issued a new strategy in 2018 that called for taking "action in cyberspace during day-to-day competition to preserve U.S. military advantages and defend U.S. interests."⁶⁸

These new concepts have been put into action as the United States and its allies deployed cyber forces to support partner defenses. In a speech at the 2022 Reagan National Defense Forum, General Paul Nakasone, commander of U.S. Cyber Command and director of the NSA, recounted growing his hunt-forward team by 300 percent in 2021.⁶⁹ Similarly, the European Union activated its Cyber Rapid Response Team to help Ukraine fend off Russian cyberattacks.⁷⁰ NATO went as far as to accept Ukraine as a contributing participant in its Cooperative Cyber Defense Centre of Excellence.⁷¹ U.S. defend-forward efforts have gone beyond cyber defense to covertly remove Russian malware from computer networks around the world.⁷² What is unclear as of this writing is whether or not these defend-forward activities have also included spoiling attacks to disrupt Russian cyber capabilities.

2. "It's a Matter of Time"



Russia could be regrouping following the initial success of Ukraine's foreign-backed cyber defense or could be biding its time. The absence of a significant critical infrastructure attack using malware to date does not preclude one in the future.

First, there are indications that Russia has been working to disrupt command and control since the beginning of the war. Hours before the ground invasion began, Russia deployed malware that disrupted the Viasat satellite system and led to over 30,000 internet connections going down temporarily across Europe, including 5,000 wind turbines.⁷³ SpaceX's leadership claims that the company's Starlink network has resisted multiple Russian cyberattacks since the capability was deployed to Ukraine.⁷⁴ More recently, there are reports of Russian cyber operations trying to penetrate Delta, a unique Ukrainian military intelligence and targeting fusion software.⁷⁵

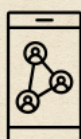
Second, since the beginning of the war, there have been reports of malware discovered on critical infrastructure in countries supporting Ukraine with foreign military assistance. In the United States, Russian malware was discovered on critical infrastructure linked to generating and providing electricity early in the conflict, which, if not discovered, could have been used to cause blackouts and supply disruptions.⁷⁶ The United Kingdom issued a public warning for critical infrastructure organizations about Moscow's increased efforts to target critical infrastructure since the start of the war in Ukraine.⁷⁷ Poland is a frequent target, with logistics suppliers commonly put at risk, primarily with ransomware.⁷⁸



Russia has also been implicated in efforts to develop even more sophisticated tool kits. These measures include new classes of industrial control malware designed to disrupt, degrade, or destroy critical infrastructure, similar to the effects seen historically in the Stuxnet attack on Iranian nuclear facilities first discovered in 2010 and the BlackEnergy attacks that disrupted Ukraine's electrical grid in 2015.⁷⁹ This activity parallels increased activity by Russian cybercriminal networks targeting critical infrastructure.⁸⁰ There are also reports that Russia is developing a new capability combining electronic warfare, signals intelligence, and cyber capabilities focused on targeting critical infrastructure and "life support systems."⁸¹ This focus on sabotaging critical infrastructure is a key component of Russian military theory and the concept of "strategic operation for the destruction of critically important targets," also known as SODCIT.⁸²

Yet Russian efforts to use cyberspace to degrade Western support or Ukrainian military capabilities have largely failed to meet expectations to date. Three reasons stand out. First, it may be that the defense is dominant in cyberspace. Moscow finds itself up against not just Ukraine but a global network of public and private cybersecurity professionals, limiting the extent to which it can exploit cyberspace. Second, there might be a tendency toward threat inflation in cyber reporting that makes Russian efforts look more sophisticated and robust than they actually are. Even the Viasat attack did not have a significant impact in Ukraine, according to Viktor Zhora, deputy chairman and chief digital transformation officer at the State Service of Special Communication and Information Protection (SSSCIP) of Ukraine.⁸³ Third, there might be an even more simple logic: critical infrastructure in Ukraine can be degraded using cruise missile strikes, allowing Russia to reserve exquisite malware in case the war escalates to involve direct combat with the West. In other words, there might be escalation dynamics in cyberspace that restrain states from launching an all-out cyberattack campaign on a rival great power even amid a proxy war.

3. "It's a Different War"



Russia might be waging a different kind of cyberwar focused less on taking down critical infrastructure and more on limiting the coalition supporting Ukraine. This information warfare strategy seeks to sow chaos and cause doubt and confusion in a manner consistent with legacy Soviet ideas about active measures and reflexive control.⁸⁴

Microsoft reported Russian network intrusion efforts in over 100 organizations in over 40 countries beyond Ukraine.⁸⁵ Many of these efforts involve "Advanced Persistent Manipulator (APM) teams" linked to the Kremlin who specialize in planting false narratives across social media in a manner "similar to the pre-positioning of malware."⁸⁶ Russian cyber operators continue to conduct low-level disruptions against targets in its near abroad, targeting Ukraine and states supporting Ukraine. A recent attack by the Sandworm group, attributed to the Russian GRU, targeted Ukinform, the national news agency of Ukraine.⁸⁷ *Politico* notes that Russia has sought to terrorize the Ukrainian civilian population after failing to leverage cyber operations on the battlefield.⁸⁸

Outside of Ukraine, Russian-linked actors have used low-level attacks to disrupt websites,

There might be escalation dynamics in cyberspace that restrains states from launching an all-out cyberattack campaign on a rival great power even amid a proxy war.

consistent with a cyber approach to political warfare.⁸⁹ Lithuania was targeted after placing restrictions on Russia cargo moving into Kaliningrad.⁹⁰ Many Russian-aligned threat groups have joined the chaos, targeting Norway, Finland, Estonia, and Latvia.⁹¹

Globally, Russia uses cyberspace to wage what researchers at the Atlantic Council call “narrative warfare.”⁹² These operations focus on eroding global confidence in Ukraine.⁹³ Unlike traditional cyber intrusions, the goal is either to cause chaos or to shape public attitudes toward the conflict using computational propaganda. These methods include creating fake social media accounts, using bots, and targeting content prompts to unique user groups to change public attitudes.⁹⁴ For example, consider Moscow’s cyber-enabled information operations across Africa that accelerated after the Russian invasion in 2022. As early as 2019, researchers identified a cluster of Facebook pages tied to the Wagner Group that were active in Libya, the Central African Republic, Sudan, the Democratic Republic of Congo, Madagascar, and Mozambique.⁹⁵ The operation showed a high degree of sophistication, including using local subcontractors and native speakers, adapting messages to unique content forms such as short videos and contests, and using Google Forms to solicit feedback.⁹⁶ These operations accelerated after the 2022 invasion of Ukraine, with new groups such as Russosphere promoting Kremlin-linked propaganda on social media calibrated to diverse audiences across Africa.⁹⁷ These social media outreach efforts complement more traditional propaganda approaches linked to platforms such as RT, which has expanded its coverage across Africa since the start of the war.⁹⁸

From Strange Patterns to Alternative Futures

When combined with the empirical trends of Russian cyberattacks against Ukraine, these three logics provide the foundation for imagining how the cyber war in Ukraine—if not beyond—could evolve over the next 12 to 36 months.

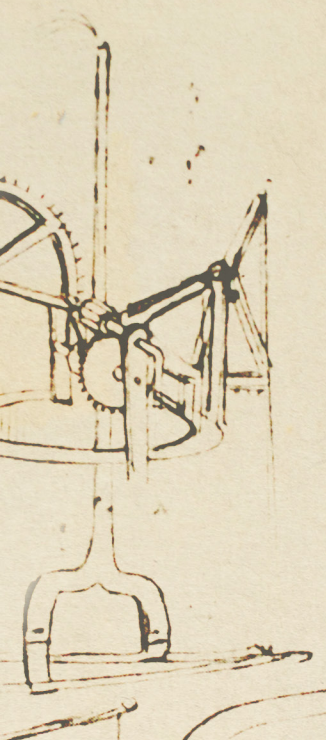
Cyber Stalemate: In the future, the defense remains dominant, limiting offensive cyber campaigns in Ukraine.



Leaders in Russia find progress on the cyber front as stalled as the battlefield. While trench lines, rivers, and concrete-reinforced fighting positions make maneuvering difficult in the real world, a mix of private sector firms and governments thwart cyber offensives in cyberspace. Moreover, Russian efforts to expand the scope of cyberattacks beyond Ukraine yield few long-term results and make Russia an international pariah on par with North Korea. Russian criminal groups thrive, increasing ransomware campaigns and “crime-as-a-service” campaigns globally, but Moscow proves unable to align cyber operations with its political objectives of winning the war in Ukraine and establishing Russian hegemony in its near abroad.

The wave of foiled Russian cyber offenses leads to a new debate about the efficacy of cyber operations as an instrument of war. The debate pits the United States, where the military and intelligence community back expanding investments in cyber capabilities despite Russian setbacks, against partners in Europe, many of whom want to see broader prohibitions against cyber operations and to pool data on attacks and vulnerabilities to increase security. These efforts are complicated by stalled legislation and executive action in the United States seeking to incentivize the private sector to report on network intrusions. The net result is that the United States and its partners are increasingly at odds over cyberspace and that there is no unity of effort in cybersecurity efforts between the public and private sectors. State cyber is limited beyond espionage, but criminal activity rises, leading to a loss of confidence in the ability or interest of the U.S. federal government to defend cyberspace.

China watches the debates and continues to invest in a mix of domestic surveillance and cyber support for firepower strike concepts. The People’s Liberation Army (PLA) focuses more on



intelligence collection and targeting and refining ways of integrating cyber, electronic warfare, and signals intelligence to avoid Moscow's fate. More troubling, Russia's failure to integrate cyber operations with its military campaign pushes Beijing to increase its investments in weaponizing space. PLA military leaders assess that a mix of kinetic and non-kinetic effects against U.S. and partner nation satellite constellations will prove more reliable than terrestrial network intrusions and hard-to-contain malware attacks.

War Comes Home: In the future, Russia escalates and unleashes a wave of critical infrastructure attacks.

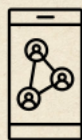


With battlefield progress stalling and Western aid continuing to flow to Kyiv, Moscow authorizes a new campaign to attack critical infrastructure in states backing Ukraine. After years of experimentation in the wild, Russian cyber operators craft tool kits that exploit industrial control systems linked to energy production and transmission, transportation systems, wastewater treatment, and a wide range of factory processes. Whereas the earlier Viasat campaign knocked out 5,000 wind turbines, the latest effort leaves millions with intermittent access to power and water across Europe and the United States for 10 days. The result is widespread panic that leaves hundreds dead in the depths of winter. The economic fallout is worse, with widespread stock market crashes and currency runs. Business leaders are angry with Western intelligence and military leaders after it is revealed that components of the Russian cyber campaign were based on malware developed by the U.S. intelligence community that Moscow repurposed.

Facing widespread public pressure, the U.S. president retaliates against Russia. U.S. cyber operations cripple critical infrastructure across Russia and create a widespread humanitarian disaster despite efforts to conduct precision targeting of facilities linked to political elites and the military. The spillover effects lead to widespread economic fallout and further stress already weak infrastructure across Russia, causing a temporary rally-around-the-flag effect. Russian citizens back retaliation.

In response to the cyberattacks, Russia places its nuclear forces on alert and deploys additional delivery systems to Belarus. Russian submarines cut key fiber-optic cables, leading to the degradation of information exchange, such as global communication and key anti-submarine early warning systems. Through back channels, Moscow signals that it intends to use nonstrategic nuclear weapons in Ukraine and will respond if the United States or any NATO member intervenes. The United States is forced to increase its nuclear alert levels, pushing the world into the most dangerous strategic crisis since the 1962 Cuban Missile Crisis. Pundits dub the standoff the "Cyber Missile Crisis."

Digital Lies: In the future, Russian cyber efforts create a backlash against the United States' image abroad.



Despite military setbacks in Ukraine and dissent at home, attitudes toward Russia across the Global South are increasingly positive. The use of troll farms, easy access to RT in Africa, and computational propaganda successfully create an image of Moscow as a victim of Western neo-imperialism. Putin is seen in these narratives as more of a twenty-first-century Che Guevara than an aging strongman. The barrage of global propaganda complicates U.S. development programs and leads to widespread protests outside U.S. embassies abroad. Chinese Communist Party intermediaries amplify these efforts and spread the discontent to Southeast and Central Asia as well as Latin America.

At home, the global wave of propaganda finds inroads on both the left and right of the U.S.



political spectrum. Propaganda tailored to right-wing audiences stresses Russia as a defender of Christianity and a bulwark stopping a “woke West” from triggering the collapse of civilization. On the left, the social media-tailored messages speak to nonintervention and a need to divest from military power in favor of social spending at home. These messages also seek to link the framing of Washington as a neo-imperial power to historic grievances inside the United States.

The campaigns are accelerated by widespread access to generative artificial intelligence (AI), leading to a wave of deepfakes and AI-written content online. Absent public or private sector policies to moderate content, the barrage of content overwhelms social media. Public trust in governing institutions continues its long-term decline and spreads to a larger sense of cynicism in U.S. society.

Policy Implications


The empirical evidence combined with the scenarios suggests a need to expand public-private partnerships and other collective defense mechanisms in cyberspace while developing new approaches to counter-influence operations and competition in the information environment. These recommendations, though developed independently and prior to its publication, match priorities outlined in the 2023 National Cyberspace Strategy.

Recommendation 1: Increase Public-Private Partnerships Supporting Cyber Defense

It is not enough to secure critical U.S. intelligence and military networks. Modern societies live through complex networks that cross the public and private sectors. The easier it is to create pooled data and common standards, the harder it will be for adversaries to compromise security. This is equivalent to the old military adage of “moving with the terrain.” If the terrain (i.e., cyberspace) is defined by scalable networks connecting diffuse groups, then making it easier for these groups to coordinate defense will make it harder for any one actor to conduct offensive action.

In practical terms, this logic means that the more incentives the U.S. government can offer for public-private sector collaboration, the more likely cyber defense will hold against future attacks. For example, what if the companies that moved to help countries and societies under siege such as Ukraine were given tax credits or at least allowed to factor the labor hours used as a tax write-off? What if the U.S. government created a new category of grants or contract vehicles, such as indefinite delivery, and indefinite quantity contracts (IDIQs), that allowed the private sector to rapidly surge for supporting key U.S. partners and allies during a crisis? The ends and ways are clear: bolster cyber defenses through increased public-private collaboration. What is less clear is the optimal means for doing so, which will likely require a creative mix of inducements and policy changes similar to those proposed by the U.S. Cyberspace Solarium Commission.

Second, increasing public-private partnership should leverage clear, transparent pooled data on cyber threats. While the U.S. government is making progress on sharing threat information, the process could go much further. Just as the private sector relies on economic and weather data collected by the U.S. government, the same should apply to cyberspace, with the U.S. government maintaining a pool of credible data continually updated by data scientists. This data pool should anonymize entity names (e.g., businesses, nonprofits, and government agencies), similar to established practices with the Federal Aviation Administration Aviation Safety Reporting Program, and use a common typology, as seen in the MITRE ATT&CK framework. Without this common reference data set, the U.S. government and the private sector are as blind as financial firms were before government reporting of inflation and employment statistics.



Pooled data is a public good that can help public-private sector collaboration. Understanding attack trends over time will help cybersecurity professionals determine when to update networks and the best mix of defenses to ensure continuity of operations. With this information, the U.S. government can then determine where and how best to defend forward, prioritizing more exquisite cyber operations against threats yet to be mitigated by increased public-private sector coordination.

Recommendation 2: Increase Diplomatic Engagement around Cyber Defense and Shared Intelligence

Similar to working with the private sector, the U.S. government should expand efforts to coordinate with partners and allies to secure cyberspace. Recommendations like this are easy to say but hard to implement, requiring coordination across multiple agencies by, with, and through multiple partners. While the Department of State will play the leading role, it must work with other departments, such as the Department of Homeland Security, the Department of Justice, and multiple elements within the military and intelligence community, to coordinate partner outreach activities.

The resiliency of Ukrainian networks has been in part related to actions taken prior to the conflict to support developing and implementing a national cyber strategy. Ukraine's strength in cyber defense has illustrated the critical role played by not just the private sector but also foreign governments in helping Kyiv prepare for the increase in cyber intrusions during the opening stages of the war.⁹⁹

There are two primary areas to focus on with diplomatic outreach in support of cybersecurity: information sharing and interoperability. With respect to information sharing, the U.S. government should accelerate efforts to share knowledge of vulnerabilities with its partners. Too often, governments withhold information out of a desire to protect sources and methods used to gain the insight or, more insidiously, because the vulnerability data is linked to exploits currently in use by said government. These limitations, while valid, tend to prevent sharing of timely information on cyber vulnerabilities with partners and allies. They also create bureaucratic barriers and a culture of "no" that limits trust among key partners, often leading to delayed collection and imbalanced understanding of the cyber operational environment that discourages collective defense and coordination. It is also worth pointing out that without a central data repository, there is no single, verified repository tracking cyberattacks using a common framework. Even if it exists on classified networks, which these authors doubt, the bureaucratic barriers to sharing limit timely access or updates, often leaving even the intelligence community dependent on third-party vendors, such as threat intelligence firms.

Second, diplomatic outreach should build interoperability with key partners and allies by increasing the number of crisis simulations and cyber games used to develop a common understanding of how best to respond to coordinate cyber defenses, including incident response and consequence mitigation. Organizations such as the Cybersecurity Infrastructure and Security Agency (CISA) have a proven track record of developing and running major cyber exercises for federal, state, and local agencies. These efforts should be expanded to include international programs facilitated by the Department of State. These games would explore critical infrastructure attacks occurring simultaneously in multiple countries and how best to coordinate cyber defenses and incident response. These games would respond to the most dangerous course of action: that a rogue state such as Russia successfully degrades critical infrastructure globally. Given the targeting data seen above, this campaign would likely target private sector systems and seek to hold a state hostage through the suffering of its people (i.e., deterrence by punishment) as part of an escalating

crisis. Given recent revelations about China's probing of critical infrastructure networks globally, this finding extends well beyond coordinating defense against Russia.¹⁰⁰

Recommendation 3: Reassess How to Counter Cyber-Enabled Information Operations

Observations of the first year of the war in Ukraine suggest that it is easier to defend against malware than lies. However, the U.S. government has yet to develop a credible, dynamic response to cyber-enabled information operations and computational propaganda. Efforts such as the Department of State's Global Engagement Center are a step in the right direction but are underfunded and lack the authorities to counter misinformation, disinformation, and malinformation at machine speed.

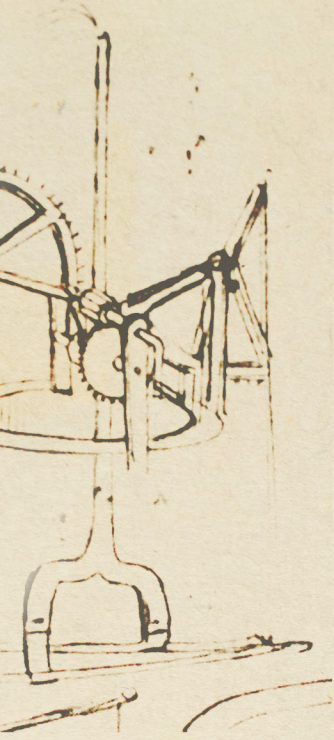
The challenges of countering global propaganda are so large that no single agency or approach is likely to address them. Therefore, the U.S. Congress should charter a new congressional commission to study how best to combat misinformation as it relates to the larger U.S. national security strategy and challenge of existing legislated authorities. Prior commissions such as the U.S. Cyberspace Solarium Commission are an example of how to catalyze change as it relates to securing cyberspace and can serve as a model.

Conclusion

The use of cyberspace to connect battle networks, support intelligence, and exchange information is here to stay. Of note, it took less time for the communication technology to become ubiquitous in war than it did for the printing press to give way to written military orders. Yet the shape of modern war is reinforcing previous academic work skeptical of the term "cyberwar" and the extent to which states have successfully integrated the use of malware, which may be better suited for espionage than battlefield tool kits. Combined arms warfare is hard. Cyber combined effects are even more difficult and prone to uneven results, opportunity costs, and the perennial fog and friction that hang over the use of violence in pursuit of political objectives.

It is dangerous to use any one case to generalize the character of war. Yet the scale and stakes of the war in Ukraine make it a crucial case for understanding the future of war. Because it is hard to imagine any future conflict where cyberspace does not play some supporting role across the levels of war, failing to analyze how great powers such as Russia apply cyber power risks missing key trends.

The mix of empirical assessment and alternative futures reviewed here suggest that cyber operations will likely prove better suited for shaping strategic interactions—whether through espionage or propaganda campaigns—than determining tactical outcomes. As with electronic warfare and signals intelligence, even when cyber operations support the art of battle, it will be indirectly and through altering the balance of information between opposing forces. Even here, the decision to employ exquisite cyber capabilities will be subject to intelligence and technical gain/loss analysis as commanders at different levels in the chain of command seek to preserve capability and balance exploitation with access. Put simply, the rush to use cyber access for a battlefield effect risks losing operational and strategic access. There is a commitment problem hanging over cyber operations: fear of future loss limits current use. This makes the idea of "cyber call for fire" at the battalion and company level a prospect that will always be subject to restrictions based on rules of engagement, authorities, and gain/loss considerations in a manner that structurally limits its responsiveness. This logic adds to preference for substituting easier-to-measure physical effects such as artillery and missile strikes. Why hack what you can destroy?



The strategic logic of cyberspace is harder to gauge. There still is the prospect that Moscow has held back significant cyber capabilities to hold Western critical infrastructure at risk as a strategic deterrent. Even if this is true, a cursory look at Ukraine shows that previous efforts to use cyber operations to degrade critical infrastructure have produced only limited, temporary results. The prospect is further questionable given the balance of offense and defense in cyberspace as multiple countries and firms race to search for intrusions. Last, even though cyberspace is critical to modern political warfare and propaganda campaigns, the extent to which the population continues to be captured by subtle lies and deepfakes is unknown. The future could prove that distracted citizens around the world prove as susceptible to cyber-enabled influence campaigns as they are to data-driven marketing. Alternatively, people will begin to adapt, making them more resilient to the flood of lies that accompanies all war, but also likely more cynical and prone to mistrust. ■

Grace B. Mueller, PhD is a postdoctoral fellow at the Army Cyber Institute. **Benjamin Jensen**, PhD is the senior fellow for future war, gaming, and strategy in the International Security Program at the Center for Strategic and International Studies (CSIS) and a professor in the Marine Corps University, School of Advanced Warfighting. **Brandon Valeriano**, PhD is a distinguished senior fellow at the Krulak Center for Innovation in the Marine Corps University. He previously served as a senior adviser to the Cyberspace Solarium Commission and is currently a senior adviser to Solarium 2.0. **Ryan C. Maness**, PhD is an assistant professor in the Defense Analysis Department at the Naval Postgraduate School (NPS). He is also the director of the DOD Information Strategy Research Center at NPS. **Jose M. Macias** is a research assistant with the International Security Program at CSIS.

The views expressed herein are those of the authors, and do not represent the policies of the U.S. government, U.S. Department of Defense, U.S. Department of the Navy, or the U.S. Marine Corps.

This report was made possible through generous support from the Carnegie Corporation of New York.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2023 by the Center for Strategic and International Studies. All rights reserved.

ENDNOTES

- 1 This count does not include multiple conflicts in the Caucasus that are internal to the Russian state or the Transnistria War and Tajik Civil War since neither border the Russian state after the collapse of the Soviet Union. Russia launched cyber operations against Estonia (primarily 2007), Georgia (primarily 2009), Lithuania (various), Poland (various), and Ukraine (pre-2014, 2014–2020, 2021–2022).
- 2 William Courtney and Peter A. Wilson, “If Russia Invaded Ukraine,” RAND, December 8, 2021, <https://www.rand.org/blog/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html>; and Maggie Miller, “Russian invasion of Ukraine could redefine cyber warfare,” *Politico*, January 28, 2022, <https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051>.
- 3 See “Thunder Run” in David Cattler and Daniel Black, “The Myth of the Missing Cyberwar: Russia’s Hacking Succeeded in Ukraine – and Poses a Threat Elsewhere, Too,” *Foreign Affairs*, April 6, 2022, <https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar>.
- 4 For more thorough review of “Thunder Runs” see Maj. Nicolas Fiore, “The 2003 Battle of Baghdad A Case Study of Urban Battle during Large-Scale Combat Operations,” *Army University Press*, September 2020, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Fiore-Battle-Baghdad/>.
- 5 Dustin Volz, “Russian hackers tracked Ukrainian artillery units using Android implant: report,” Reuters, December 21, 2016, <https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU>.
- 6 Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” *International Security* 38, no. 2 (2013): 41–73, doi:10.1162/ISEC_a_00136; Erik Gartzke and Jon R. Lindsay, “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace,” *Security Studies* 24, no. 2 (2015): 316–48, doi:10.1080/09636412.2015.1038188; Benjamin Jensen, ““The Cyber Character of Political Warfare,”” *The Brown Journal of World Affairs* 24, no. 1 (2017): 159–72, <https://bjwa.brown.edu/24-1/Benjamin-jensen-the-cyber-character-of-political-warfare/>; Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford, UK: Oxford University Press, 2018); Erica D. Borghard and Shawn W. Lonergan, “The Logic of Coercion in Cyberspace,” *Security Studies* 26, no. 3 (2017): 452–81, doi:10.1080/09636412.2017.1306396; and Joshua Rovner, “What Is an Intelligence Contest?,” *Texas National Security Review*, 3, no. 4, Fall 2020, <https://repositories.lib.utexas.edu/bitstream/handle/2152/83955/TNSRVol3Iss4Rovner.pdf?sequence=2>.
- 7 Benjamin Jensen, Brandon Valeriano, and Ryan Maness, “Fancy bears and digital trolls: Cyber strategy with a Russian twist,” *Journal of Strategic Studies* 42, no. 2 (2019): 212–34, doi:10.1080/01402390.2018.1559152.
- 8 U.S. Department of Defense, *Joint Publication 3-0: Joint Operations* (DOD, January 2017), https://irp.fas.org/doddir/dod/jp3_12.pdf.
- 9 Ibid.
- 10 Benjamin Jensen and J.D. Work, “Cyber Civil-Military Relations: Balancing Interests on the Digital Frontier,” *War on the Rocks*, September 4, 2018, <https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/>.
- 11 Ryan C. Maness et al., “Expanding the Dyadic Cyber Incident and Dispute (DCID) Dataset: Cyber Conflict,” *Cyber Defense Review*, forthcoming.
- 12 Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in*

the International System (Oxford, UK: Oxford University Press, 2015). In addition, the term cyber incident has a specific definition in U.S. legal code, “an occurrence that—(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or information system; or (B) constitutes a violation of imminent threat of violation of law, security, policies, security procedures, or acceptable use policies.” See “44 U.S. Code § 3552- Definitions,” Cornell Law School, <https://www.law.cornell.edu/uscode/text/44/3552>.

- 13 Joshua Rovner, “Warfighting in Cyberspace,” *War on the Rocks*, March 17, 2021, <https://warontherocks.com/2021/03/warfighting-in-cyberspace/>.
- 14 Jan Kallberg, “Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations,” *The Cyber Defense Review* 1, no. 1 (2016): 124, <https://www.jstor.org/stable/26267302>.
- 15 Ibid.
- 16 Ibid.
- 17 Lucas Kello, “Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” *International Security* 38, no. 2 (2013): 7–40, <https://www.jstor.org/stable/24480929>.
- 18 Amit Sharma, “Cyber Wars: A Paradigm Shift from Means to Ends,” *Strategic Analysis* 34, no. 1 (2010): 65, doi:10.1080/09700160903354450.
- 19 Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 1.
- 20 Ibid., 4.
- 21 Kallberg, “Strategic Cyberwar Theory,” 125.
- 22 Keith Alexander, “Cyber warfare in Ukraine poses a threat to the global system,” *Financial Times*, February 15, 2022, <https://www.ft.com/content/8e1e8176-2279-4596-9c0f-98629b4db5a6>.
- 23 Cattler and Black, “The Myth of the Missing Cyberwar.”
- 24 Keir Giles, “Putin does not need to invade Ukraine to get his way,” Chatham House, December 21, 2021, <https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way>.
- 25 Tammi Biddle, *Rhetoric and Reality: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945* (Princeton, NJ: Princeton University Press, 2002).
- 26 Jason Healey, “Preparing for Inevitable Cyber Sunrise,” *War on the Rocks*, January 12, 2022, <https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/>.
- 27 Rebecca Klar, “CISA director: US needs to be vigilant, ‘keep our shields up’ against Russia,” *The Hill*, January 5, 2023, <https://thehill.com/policy/technology/3801077-cisa-director-us-needs-to-be-vigilant-keep-our-shields-up-against-russia/>.
- 28 Borghard and Lonergan, “The Logic of Coercion in Cyberspace”; Gartzke, “The Myth of Cyberwar”; and Joseph S. Nye, “Deterrence and Dissuasion in Cyberspace,” *International Security* 41, no. 3 (2017): 44–71, doi:10.1162/ISEC_a_00266.
- 29 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 (Summer 2022): 113–26, doi:10.26153/tsw/42073.
- 30 Christopher Bronk, Gabriel Collins, and Dan Wallach, “Cyber and Information Warfare in

Ukraine: What Do We Know Seven Months In?," Baker Institute, September 6, 2022, <https://www.bakerinstitute.org/research/cyber-and-information-warfare-ukraine-what-do-we-know-seven-months>.

- 31 Brandon G. Valeiano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Cyber Restraint," Cato Institute, Policy Analysis 862, January 15, 2019, <https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint>.
- 32 Gartzke and Lindsay, "Weaving Tangled Webs."
- 33 Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (Athens: University of Georgia Press, 2016), https://getd.libs.uga.edu/pdfs/brantly_aaron_f_201212_phd.pdf; Rovner, "What Is an Intelligence?"; and Valeriano, Jensen, and Maness, *Cyber Strategy*.
- 34 Valeriano and Jensen, "The Myth of the Cyber Offense"; Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review*, 2019: 267–87, https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.
- 35 Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (Winter 2016/17), 72–109, doi:10.1162/ISEC_a_00267.
- 36 Mark Montgomery et al., *Cyberspace Solarium Commission Report* (Washington, DC: March 2020), <https://www.solarium.gov/report>; Brandon Valeriano and Benjamin M. Jensen, "Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report," 13th International Conference on Cyber Conflict (CyCon), Tallin, Estonia, 2021, 189–214, doi:10.23919/CyCon51939.2021.9467806. Of note, the Ukrainian government sent an official delegation to meet with the senior research director in the fall of 2021 and claimed the layered deterrence concept and commission report were blueprints as they prepared to counter Russian cyber operations targeting Ukraine.
- 37 Valeriano, Jensen, and Maness, *Cyber Strategy*; and Jensen, Valeriano, and Maness, "Fancy bears and digital trolls."
- 38 Ryan Maness and Brandon Valeriano, *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power* (New York, NY: Springer, 2015).
- 39 Ibid.
- 40 See the complete NIST definition: National Institute of Standard and Technology, [https://csrc.nist.gov/glossary/term/information_operations#:~:text=Definition\(s\)%3A,Also%20called%20IO](https://csrc.nist.gov/glossary/term/information_operations#:~:text=Definition(s)%3A,Also%20called%20IO).
- 41 See John Hultquist, "Sandworm Team and the Ukrainian Power Authority Attacks," Mandiant, August 23, 2022, <https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team>.
- 42 See Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
- 43 See Andrea Vittorio, "Merck's \$1.4 Billion Insurance Win Splits Cyber From 'Act of War,'" Bloomberg Law, January 19, 2022, <https://news.bloomberglaw.com/privacy-and-data-security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war>.
- 44 Charlie Smart, "How the Russian Media Spread False Claims About Ukrainian Nazis," *New York Times*, July 2, 2022, <https://www.nytimes.com/interactive/2022/07/02/world/europe/ukraine->

nazis-russia-media.html.

- 45 Christopher A. Bail et al., “Assessing the Russian Internet Research Agency’s Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017,” *Proceedings of the National Academy of Sciences* 117, no. 1 (2020): 243–50, doi:10.1073/pnas.1906420116.
- 46 See Ellen Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms,” *Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
- 47 See David E. Sanger, Nicole Perlroth, and Eric Schmitt, “Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit,” *New York Times*, December 14, 2020, <https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html>.
- 48 See David E. Sanger and Nicole Perlroth, “Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity,” *New York Times*, May 14, 2021, <https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html>.
- 49 Maness et al., “Expanding the Dyadic Cyber Incident and Dispute (DCID) Dataset: Cyber Conflict,” Forthcoming.
- 50 For a complete severity scale overview see Maness et al., “Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 2.0,” July 2022, <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset>.
- 51 David Singer and Melvin Small built on earlier work by Lewis Frye Richardson and Quincy Wright to pioneer the scientific study of war. See J. David Singer and Melvin Small, *Wages of War, 1816-1965: A Statistical Handbook* (New York: John Wiley & Sons, 1972). Another groundbreaking effort was the International Crisis Behavior (ICB) data set, which used similar statistical methods but combined diplomatic history and kept case inventories. On the ICB, see Michael Brecher and Jonathan Wilkenfeld, *A Study of Crisis* (Ann Arbor, MI: University of Michigan Press, 1997).
- 52 The authors recognize that this does not include all cyberattacks that have occurred, especially given that the most recent SSSCIP report stated that the Computer Emergency Response Team of Ukraine (CERT-UA) has detected 1,123 cyberattacks between February 24, 2022, and August 24, 2022. There is a significant difference between an isolated cyberattack and cyber operations conducted by the Russian government or its proxy entities, which tend to comprise many different cyberattacks and take the form of campaigns involving multiple intrusions.
- 53 Sean Lyngaas, “Russian hacking in Ukraine has been extensive and intertwined with military operations, Microsoft says,” *CNN*, April 27, 2022, <https://www.cnn.com/2022/04/27/europe/russia-cyberattacks-ukraine-war-microsoft/index.html>.
- 54 James Andrew Lewis, “Cyber War and Ukraine,” *CSIS White Papers*, June 16, 2022, <https://www.csis.org/analysis/cyber-war-and-ukraine>.
- 55 Lennart Maschmeyer and Nadiya Kostyuk, “There Is No Cyber ‘Shock and Awe’: Plausible Threats in the Ukrainian Conflict,” *War on the Rocks*, February 8, 2022, <https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/>; and “The Head of the GCHQ says Vladimir Putin is losing the information war in Ukraine,” *The Economist*, August 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>.
- 56 Christopher Miller, Mark Scott, and Bryan Bender “UkraineX: How Elon Musk’s space satellites

changed the war on the ground,” *Politico*, June 8, 2022, <https://www.politico.eu/article/elon-musk-ukraine-starlink/>.

- 57 Brad Smith, “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft, June 22, 2022, <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.
- 58 Ibid.
- 59 Katherine Tangelakis-Lippert, “Amazon helped the Ukrainian government and economy using suitcase-sized hard drives brought in over the Polish border: ‘You can’t take out the cloud with a cruise missile,’” *Business Insider*, December 18, 2022, <https://www.businessinsider.com/amazon-saved-the-ukrainian-government-with-suitcase-sized-hard-drives-2022-12>.
- 60 Russ Mitchell, “How Amazon put Ukraine’s ‘government in a box’ – and saved its economy from Russia,” *Los Angeles Times*, December 15, 2022, <https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data>.
- 61 Matthew Prince, “Steps we’ve taken around Cloudflare’s services in Ukraine, Belarus, and Russia,” Cloudflare, March 7, 2022, <https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/>.
- 62 Karl Greenberg, “With political ‘hacktivism’ rising, Google offers Project Shield to fight DDOS attacks,” *TechRepublic*, March 28, 2023, <https://www.techrepublic.com/article/google-launches-project-shield/>.
- 63 Emma Schroeder and Sean Dack, *A Parallel Terrain: Public-Private Defense of Ukrainian Information Environment* (Washington, DC: Atlantic Council, 2023), <https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/>; and Stephanie Pell, “Private Sector Cyber Defense in Armed Conflict,” *Lawfare*, December 1, 2022, <https://www.lawfareblog.com/private-sector-cyber-defense-armed-conflict>.
- 64 Montgomery et al., *Cyberspace Solarium Commission Report*; and Nick Beecroft, “Evaluating the International Support to Ukrainian Cyber Defense,” *Carnegie Endowment for International Peace*, November 3, 2022, <https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322>.
- 65 “U.S. Support for Connectivity and Cybersecurity in Ukraine,” U.S. Department of State, May 10, 2022, <https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/>.
- 66 EEAS Press Team, “Ukraine and EU held the second round of UA-EU cybersecurity dialogue,” European Union, September 2, 2022, https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en.
- 67 Sean Lawson, “DOD’s “First” Cyber Strategy is Neither First, Nor a Strategy,” *Forbes*, August 1, 2011, <https://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/?sh=3801165419cb>.
- 68 Gary P. Corn and Emily Goldman, “Defend Forward and Persistent Engagement” in Jack Goldsmith, ed., *The United States Defend Forward Cyber Strategy* (New York: Oxford University Press, 2022), <https://academic.oup.com/book/41393/chapter-abstract/352684202?redirectedFrom=fulltext>. For an overview of the strategy, see Nina Kollars and Jacquelyn Schneider, “Defending Forward: The 2018 Cyber Strategy Is Here,” *War on the Rocks*, September 20, 2018, <https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/>. The concept is linked to cyber persistence theory, see Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022).

- 69 The team grew from 10 to 39 people and was led by a Marine Maj. David Vergun, “Partnering with Ukraine on Cybersecurity Paid Off, Leaders Say,” U.S. Department of Defense, December 3, 2022, <https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/>.
- 70 Laurens Cerulus, “EU to mobilize cyber team to help Ukraine fight Russian cyberattacks,” *Politico*, February 21, 2022, <https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/>.
- 71 Suzanne Smalley, “Ukraine, looking to fortify itself against Russian attacks, admitted to NATO cyber center,” *Cyberscoop*, March 4, 2022, <https://cyberscoop.com/ukraine-admitted-nato-ccdcoe/>.
- 72 Kate Conger and David Sanger, “U.S. Says It Secretly Removed Malware Worldwide, Pre-empting Russian Cyberattacks,” *New York Times*, August 6, 2022, <https://www.nytimes.com/2022/04/06/us/politics/us-russia-malware-cyberattacks.html>.
- 73 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/>.
- 74 Ed Browne, “Elon Musk Says Starlink Has Resisted Hacking Attempts From Russia ‘So Far,’” *Newsweek*, May 11, 2022, <https://www.newsweek.com/elon-musk-starlink-resisted-hacking-attempts-russia-1705495>.
- 75 Eduard Kovacs, “Ukraine’s Delta Military Intelligence Program Targeted by Hackers,” *Security Week*, December 20, 2022, <https://www.securityweek.com/ukraines-delta-military-intelligence-program-targeted-hackers/>.
- 76 Maggie Miller, “Russian-linked malware was close to putting U.S. electric, gas facilities ‘offline’ last year,” *Politico*, February 23, 2023, <https://www.politico.com/news/2023/02/14/russia-malware-electric-gas-facilities-00082675>.
- 77 Ionut Arghire, “UK Warns of Russian Hackers Targeting Critical Infrastructure,” *Security Week*, April 20, 2023, <https://www.securityweek.com/uk-warns-of-russian-hackers-targeting-critical-infrastructure/>.
- 78 Dan Goodin, “Microsoft links Russia’s military to cyberattacks in Poland and Ukraine,” *Ars Technica*, November 10, 2022, <https://arstechnica.com/information-technology/2022/11/microsoft-links-russias-military-to-cyberattacks-in-poland-and-ukraine/>.
- 79 On emerging industrial control system targeting, see “CHEVRONITE’s PIPEDREAM Malware Targeting Industrial Control Systems (ICS),” *Dragos*, April 13, 2022, <https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/>. On Stuxnet and BlackEnergy, see Valeriano, Jensen, and Maness, *Cyber Strategy*; and Anton Cherepanov and Robert Lipovsky, “BlackEnergy: What Do We Really Know About the Notorious Cyber Attack,” *Virus Bulletin Conference*, October 2016, <https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf>.
- 80 Mark Bowling, “Russia-Linked Ransomware Gangs Could Spark Revamped Cybersecurity Protocols in Critical Infrastructure,” *CPO Magazine* March 13, 2023, <https://www.cpomagazine.com/cyber-security/russia-linked-ransomware-gangs-could-spark-revamped-cybersecurity-protocols-in-critical-infrastructure/>.
- 81 Brian Livingston, “Dragos Analyzes Russian Programs Threatening Critical Civilian Infrastructure,” *Dragos, Intelligence Brief*, April 2023, https://hub.dragos.com/hubfs/Dragos_IntelBrief_Russian-Programs-Threatening-Critical_Infrastructure.pdf.

- 82 Michael Kofman et al., *Russian Military Strategy: Core Tenets and Operational Concepts* (Arlington, VA: Center for Naval Analysis, 2021), https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf; and Timothy Thomas, *Russian Military Thought: Concepts and Elements* (Arlington, VA: MITRE Corp, 2019), <https://www.mitre.org/news-insights/publication/russian-military-thought-concepts-and-elements>.
- 83 Kim Zetter, “Viasat Hack ‘Did Not’ Have Huge Impact on Ukrainian Military Communications, Official Says,” Substack, September 26, 2022, <https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact>.
- 84 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Macmillian, 2020); and Timothy Thomas, *Russian Military Thought*.
- 85 Smith, “Defending Ukraine: Early Lessons from the Cyber War.”
- 86 Ibid.
- 87 AJ Vicens, “Russia’s Sandworm hackers blamed in fresh Ukraine malware attack,” Cyberscoop, January 27, 2023, <https://cyberscoop.com/sandworm-wiper-ukraine-russia-military-intel/>.
- 88 Maggie Miller, “Russia’s cyberattacks aim to ‘terrorize’ Ukrainians,” *Politico*, January 11, 2023, <https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561>.
- 89 Jensen, “The Cyber Character of Political Warfare.”
- 90 Andrew Higgins, “Lithuania blames Russia cyberattacks, citing threats over cargo restrictions,” *The New York Times*, June 27, 2022, <https://www.nytimes.com/2022/06/27/world/europe/lithuania-russia-cyberattacks.html>.
- 91 Terje Solsvik, “Norway blames ‘pro-Russia group’ for cyber attack,” Reuters, June 29, 2022, <https://www.reuters.com/world/europe/norway-targeted-by-cyber-attack-security-agency-2022-06-29/>; Vilius Petkauskas, “Russia hackers target Finland parliament’s website,” CyberNews, August 10, 2022, <https://cybernews.com/cyber-war/russian-hackers-target-finland-parliaments-website/>; Andrius Sytas, “Estonia says it repelled major cyber attack after removing Soviet monuments,” Reuters, August 18, 2022, <https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/>; and Oliver Moody, “Pro-Kremlin hackers Killnet hit Latvia with biggest cyberattack in its history,” *The Times*, July 8, 2022, <https://www.thetimes.co.uk/article/pro-kremlin-hackers-killnet-hit-latvia-with-biggest-cyberattack-in-its-history-2jvmp8hk7>.
- 92 Andy Covin, ed., *Narrative Warfare: How the Kremlin and Russian news outlets justified a war of aggression against Ukraine* (Washington, DC: Atlantic Council, 2022), <https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/>.
- 93 Andy Covin, ed., *Undermining Ukraine: How the Kremlin employs information operations to erode global confidence in Ukraine* (Washington, DC: Atlantic Council, 2022), <https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/>.
- 94 Sam Woolley and Phil Howard, eds., *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (New York: Oxford University Press, 2018), doi:10.1093/oso/9780190931407.001.0001.
- 95 Michael Weiss, “Russia’s Wagner Mercenaries Have Moved Into Libya. Good Luck With That,” *Daily Beast*, September 28, 2019, <https://www.thedailybeast.com/russias-wagner-mercenaries-have-moved-into-libya-good-luck-with-that>.
- 96 “Evidence of Russia-Linked Influence Operations in Africa,” Stanford Internet Observatory,

October 2019, <https://cyber.fsi.stanford.edu/io/news/prigozhin-africa>.

- 97 Grigor Atanesian, “Russia in Africa: How disinformation operations target the continent,” BBC, February 1, 2023, <https://www.bbc.com/news/world-africa-64451376>.
- 98 Elian Peltier, Adam Satariano, and Lynsey Chutel, “How Putin Became a Hero on African TV,” *New York Times*, April 13, 2023, <https://www.nytimes.com/2023/04/13/world/africa/russia-africa-disinformation.html>.
- 99 AJ Vicens, “‘A year of cyberwar’ with Russia: An inside look from a top Ukrainian cybersecurity official,” Cyberscoop, February 27, 2023, <https://cyberscoop.com/victor-zhora-ukraine-russia-cyber-war-one-year/>.
- 100 Zeba Siddiqui and Christopher Bing, “Chinese hackers spying on US critical infrastructure, Western intelligence says,” Reuters, May 25, 2023, <https://www.reuters.com/technology/microsoft-says-china-backed-hacker-targeted-critical-us-infrastructure-2023-05-24/>.