CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

DECEMBER 2022 | CYBER CONFLICT IN THE RUSSIA-UKRAINE WAR

Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications

Jon Bateman

Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications

Jon Bateman

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Cyber Conflict in the Russia-Ukraine War

The war in Ukraine is the largest military conflict of the cyber age and the first to incorporate such significant levels of cyber operations on all sides. Carnegie's series "Cyber Conflict in the Russia-Ukraine War" represents our first offerings in what will be a long, global effort to understand and learn from the cyber elements of the Ukraine war. We welcome queries from other authors interested in contributing to this endeavor by having us publish their work. If you would like to learn more, please contact Arthur Nelson at arthur.nelson@ceip.org.

Publications in this series:

- "Evaluating the International Support to Ukrainian Cyber Defense," Nick Beecroft, November 3, 2022
- "Cyber Operations in Ukraine: Russia's Unmet Expectations," Gavin Wilde, December 12, 2022
- "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Jon Bateman, December 15, 2022

Summary

This paper examines the military effectiveness of Russia's wartime cyber operations in Ukraine,[1] the reasons why these operations have not had greater strategic impact, and the lessons applicable to other countries' military cyber efforts. It builds on previous analyses by taking a more systematic and detailed approach that incorporates a wider range of publicly available data.

A major purpose of this paper is to help bridge the divide between cyber-specific and general military analysis of the Russia-Ukraine war. Most analysis of Russian cyber operations in Ukraine has been produced by cyber specialists writing for their own field, with limited integration of non-cyber military sources and concepts. Conversely, leading accounts of the war as a whole include virtually no mention of cyber operations.[2] To begin filling the gap, this paper places Russian cyber operations in Ukraine within the larger frame of Moscow's military objectives, campaigns, and kinetic activities. Its key points:

- **Russian cyber "fires" (disruptive or destructive attacks) may have contributed modestly to Moscow's initial invasion, but since then they have inflicted negligible damage on Ukrainian targets.** Traditional jamming gave Russian forces a tactical edge in the battle for Kyiv, and it is plausible—though unconfirmed—that the cyber disruption of Viasat modems further degraded Ukrainian front-line communications. Meanwhile, Russia's large opening salvo of data deletion attacks may have amplified the general atmosphere of chaos in Ukraine, although the victim organizations reportedly suffered only limited real-world disruptions. But within the first several weeks of the war, Russian cyber fires plummeted in number, impact, and novelty. Cyber fires, although still very high relative to prewar baselines, have barely registered on the grand scale of Moscow's military ambitions and high-intensity combat operations in Ukraine.

- **Cyber fires have neither added meaningfully to Russia's kinetic firepower nor performed special functions distinct from those of kinetic weapons.** Rather than serving in a niche role, many Russian cyber fires have targeted the same categories of Ukrainian systems also prosecuted by kinetic weapons, such as communications, electricity, and transportation infrastructure. For almost all these target categories, kinetic fires seem to have caused multiple orders of magnitude more damage. While cyber fires potentially offer unique benefits in certain circumstances, these benefits have not been realized in Russia's war against Ukraine. Moscow's military strategists quickly discarded any aim of reducing physical or collateral damage or creating reversible effects in Ukraine, and Russia has gained little deniability or geographic reach from cyber operations. Likewise, Russian cyber fires have not achieved any systemic effects, and they have arguably been less cost-effective—or at least more capacity-constrained—than kinetic fires.

- **Intelligence collection—not fires—has likely been the main focus of Russia's wartime cyber operations in Ukraine, yet this too has yielded little military benefit.** Although intelligence processes are more difficult for outsiders to assess than fires, Russian artillery seems to rely on non-cyber sources of targeting intelligence (particularly uncrewed aerial vehicles or UAVs), despite earlier claims that Moscow has used malware to geolocate Ukrainian positions. Russian missile forces may have received some cyber-derived intelligence, but in the handful of known plausible cases, this intelligence does not seem to have been valuable for targeting decisions. Even influence operations, long central to Moscow's cyber doctrine, have received only minimal known support from Russian hackers. More generally, Russia's ham-fisted overall approach to the war—from its campaign planning to its occupation of seized territory—suggests that key military decisions are not guided by a rigorous all-source intelligence process.

- **While many factors have constrained Moscow's cyber effectiveness, perhaps the most important are inadequate Russian cyber capacity, weaknesses in Russia's non-cyber institutions, and exceptional defensive efforts by Ukraine and its partners.** To meaningfully influence a war of this scale, cyber operations must be conducted at a tempo that Russia apparently could sustain for only weeks at most. Moscow worsened its capacity problem by choosing to maintain or even increase its global cyber activity against non-Ukrainian targets, and by not fully leveraging cyber criminals as an auxiliary force against Ukraine. Meanwhile, Russian President Vladimir Putin and his military seem unwilling or unable to plan and wage war in the precise, intelligence-driven manner that is optimal for cyber operations. Ukraine, for its part, has benefited from a resilient digital ecosystem, years of prior cybersecurity investments, and an unprecedented surge of cyber support from the world's most capable companies and governments. Given the many factors at play, even if several had been reversed it might still not have significantly improved the overall military utility of Russian cyber operations.

- **As the war continues, Russian intelligence collection probably represents the greatest ongoing cyber risk to Ukraine.** Conceivably, Russian hackers might still have larger impact if they can collect high-value intelligence that Moscow then leverages effectively. For example, the hackers might obtain real-time geolocation data that enable the assassination of President Volodymyr Zelenskyy or the timely and accurate targeting of Ukrainian forces, particularly those with high-value Western weapons systems; conduct hack-and-leak operations revealing sensitive war information to the Ukrainian and Western public, such as Ukraine's combat losses, internal schisms, or military doubts; or collect valuable information about Kyiv's perceptions and intentions that can aid Moscow at future talks, among other scenarios. Russian cyber fires pose a less serious threat, though such attacks could multiply if Moscow directs more of its overall cyber capability toward Ukraine (at the cost of other objectives) or better leverages cyber criminals.

- **Russia's war in Ukraine offers lessons for other military cyber commands, but these must be applied to national circumstances and considered alongside a range of relevant case studies.** Russia's experience suggests that cyber fires can be usefully concentrated in a surprise attack or other major salvo, but they risk fading in relevance during larger, longer wars. Cyber intelligence collection seems to have greater potential than cyber fires to support a variety of wartime military tasks, but this probably depends on having competent analysis and decisionmaking processes and a reasonably precise "way of war." Militaries with high capability, professionalism, and readiness in both cyber and kinetic disciplines—such as the United States and Israel—have previously leveraged cyber operations to enable strikes on high-value targets. Yet even top-tier militaries seem to have the greatest cyber successes in tightly circumscribed contexts. It is therefore probably misleading to view cyberspace as a "fifth domain" of warfare equivalent in stature to land, sea, air, and space.

- **Militaries that plan for major war should ask whether they can realistically meet the high bar of producing and sustaining cyber fires at meaningful levels.** Meeting this bar may require huge standing cyber forces—perhaps many times larger than what peacetime or "gray zone" conditions require. Alternatively, militaries could develop surge capacity mechanisms (reserve forces, for example), which are challenging to implement and risk cannibalizing domestic cybersecurity. The rapid regeneration of cyber capabilities is another key hurdle. Given limited wartime cyber capacity, militaries may need to experiment with wave tactics: short bursts of intense cyber fires followed by periods of stand-down and regeneration. The more infrequent the waves, the more important it will be to coordinate closely with kinetic fires. If a cyber command is unlikely to scale dramatically and regenerate rapidly, it should perhaps not aspire to conduct sustained wartime fires in major conflict. It might instead prioritize more selective fires in peacetime, gray zone, or prewar conditions, or non-fires activities like cyber defense and intelligence collection.

- **Countries' investments in cyber intelligence collection should be matched by equally dedicated efforts to hone intelligence analysis, military planning, and strategic decisionmaking.** As cyber capabilities proliferate, countries may find themselves able to collect more information than they can accurately interpret and effectively use in wartime. In such cases, broad institutional reforms—upgrading analytic tradecraft, instilling professionalism, or combating corruption—will often have more value than further technical enhancements of cyber collection. Countries unable to implement those reforms may learn that exquisite military cyber intelligence capabilities aren't worth the effort to build. Cyber units also need to be fully integrated into all-source intelligence processes that direct them toward information needs which cannot be readily fulfilled by other means. Wartime use cases for cyber intelligence might include tracking high-value targets in real time, validating human intelligence in mission-critical situations, and acquiring very large data caches with durable, multipurpose value.

- **Cyber defenders should use the Ukraine war as a reference point to reexamine and refine prior assumptions about the particular wars they might need to fight.** Their first task is to reconsider the likely ability of prospective enemies to leverage cyber operations in conflict, given Russia's humbling experience. They should then make specific comparisons and contrasts to their own military situation. For example, China's cyber forces are probably larger than Russia's, but they have carried out far fewer cyber fires. Would they execute an even bigger and more effective cyber salvo at the outset of a Taiwan invasion, or bungle the opener due to inexperience? Taiwan is more technologically advanced than Ukraine but its island geography is in some ways more precarious. Would Taiwan's communications infrastructure prove more or less resilient? The political and commercial stakes for Western tech companies could also be quite different in a China-Taiwan war. Would such firms be equally willing to help, and could they physically do so without overland access?

- **This paper's tentative insights represent one reasonable interpretation of fragmentary, conflicting, and evolving data.** Analysts remain reliant on reports from the Ukrainian government, allied governments, cybersecurity companies, and journalists to understand Russia's cyber operations, their effects, and the larger war in Ukraine. Yet those sources have only partial knowledge, and parochial concerns inevitably shape what, when, and how information is shared. Some sources, for example, have produced fewer public reports in recent months than before. The resulting "cyber fog of war" continues to shroud even the most closely watched cyber incidents. A wider fog pervades the war as a whole, which has already undergone several distinct phases in just nine months—often developing in ways that surprise Western analysts (and others). Despite this uncertainty, governments around the world will not wait to incorporate perceived lessons learned into ongoing updates of military cyber strategies, budgets, doctrines, and plans. Analysts should offer the best assessments currently possible while acknowledging information gaps and the need to reassess over time.

How Militarily Effective Have Russia's Cyber Operations Been in Ukraine?

Since Russia invaded Ukraine on February 24, 2022, most Western commentators have downplayed the role of offensive cyber operations in Moscow's larger war effort. Analysts have called Russian cyber operations sparse, unsophisticated, ill-planned, poorly integrated with activities in other domains, ably defended by Ukraine and its foreign partners, and ultimately inconsequential when compared to the large-scale death and destruction caused by physical weapons.

Experts offer competing explanations for how and why Russian cyber operations in Ukraine have fizzled, but most agree on the core military question: cyber operations have not significantly advanced Moscow's campaign objectives. James Lewis, for example, found that "cyber operations have provided little benefit" to Russia and "failed to advance Russian goals" in the war.[3] Likewise, Nadiya Kostyuk and Aaron Brantly wrote that Russian cyber attacks "did not have any strategic impact on Ukraine's warfighting capabilities" and "do not appear to have impacted the course of the war."[4] The CyberPeace Institute, which maintains a public database of Russia's cyber operations against Ukraine, said these weren't "playing a major role in . . . tactical advances."[5] Even Microsoft—which has described Russia's wartime cyber efforts as voluminous, skillful, militarily innovative, and historically important—has reported only "limited operational impact" on Ukrainian targets.[6] The company concluded that, "at a broader level, so far [Russian cyber] attacks have failed strategically in disabling Ukraine's defenses."

Not everyone shares this perspective. Prominent dissenters include some Western government officials who believe outside analysts have underestimated Russia's wartime cyber efforts against Ukraine. The dissenting camp describes Russian cyber operations as sweeping in scale, tactically effective in key moments, and aligned with Moscow's military objectives of disrupting, confusing, and cowing the Ukrainian government, armed forces, and civilian population. David Cattler and Daniel Black, two serving intelligence officials with the North Atlantic Treaty Organization (NATO), argued in April that "cyber-operations have been Russia's biggest military success to date in the war in Ukraine."[7] Jeremy Fleming, the director of the UK's General Communications Headquarters (GCHQ), called it "a fallacy to say that cyber has not been a factor in the war in Ukraine."[8] And Matt Olsen, U.S. assistant attorney general for national security, said "we are effectively seeing a hot cyber war in Ukraine carried out by the Russians."[9]

Such disagreement stems in part from fragmentary, conflicting, and evolving information about Russia's wartime cyber operations. A case in point was the February 24 disruption of the Viasat satellite communications network by Russian military intelligence—the marquee cyber event of the war so far. The hack has attracted enormous interest due to its timing (one hour before Russian troops crossed the border), clear military purpose (to degrade Ukrainian

communications), and international spillover (disrupting connectivity in several European countries). Yet the Viasat hack's ultimate military impact has remained murky and contested. Victor Zhora, a top Ukrainian cyber leader, initially said it caused "a really huge loss in communications in the very beginning of war," which was widely understood to mean military communications specifically.[10] But a Ukrainian spokeswoman claimed, and Zhora later affirmed, there was "no information that [the hack] worsened communications within Ukraine's military."[11] This factual confusion has contributed to diametrically opposed expert assessments of the Viasat hack. Dmitri Alperovitch called it "perhaps the most strategically impactful cyber operation in wartime history," while James Lewis said it "ultimately did not provide military advantage to Russia."[12]

Even where analysts share a common set of facts about Russian hacking, they often seem to apply differing (or unclear) standards to judge military utility. Commentators of all stripes have framed Russia's cyber efforts in binary terms: either as a failure or as a success. But analysts differ in where they set the dividing line between success and failure, causing people to talk past each other. On one side are cyber skeptics who often emphasize Russian hackers' inability to paralyze Ukrainian decisionmaking and critical infrastructure via "shock and awe" tactics—a high bar indeed. On the other side are cyber proponents who tend to highlight any signs of coordination between Russian kinetic and cyber operations—no matter how inconsequential the results. Given these disparate yardsticks and shifting terms of debate, it isn't always clear what analysts are arguing about, or whether they disagree at all. For example, Ciaran Martin expressed early cyber skepticism when he warned that "the cyber domain may influence the war at the margins, but it will not decide it."[13] Cattler and Black, both cyber proponents, came to a remarkably similar conclusion: "No single domain of operations has an independent, decisive effect on the course of war."[14]

Methodology

To advance the debate, this paper divides Russian cyber operations in Ukraine into two categories, each drawn from military concepts. The first category is cyber "fires." U.S. military doctrine defines fires as the "use [of] available weapons and other systems to create a specific effect on a target."[15] Cyber fires, then, would be those cyber operations intended to disrupt, destroy, or manipulate data or systems.[16] Cyber experts sometimes call these "effects operations" or "disruptive and destructive cyber attacks." Here, the term cyber fires is meant to bring the military context into the foreground, and to invite comparisons (and contrasts) to kinetic fires.

Many assessments of Russia's cyber operations in Ukraine have focused primarily—or even exclusively—on what this paper calls cyber fires. Because of their obvious analogy to kinetic strikes, disruptive or destructive cyber attacks are often thought of as the major way for cyber forces to aid military campaigns. But militaries must do much more than carry out attacks, and cyber operations have other wartime uses. In U.S. doctrine, for example, fires are just one of seven so-called joint functions—the military tasks "common to joint operations

at all levels of warfare." The others are command and control, information, intelligence, movement and maneuver, protection, and sustainment. Although each of these has some applicability in cyberspace, this paper focuses on intelligence—particularly collection—as the second major category of interest. Intelligence collection is a well-known role for cyber operations during peacetime and gray zone conditions, but it has received less attention in the wartime context.[17]

Assessing Russia's cyber operations and their effects on the larger war in Ukraine is no simple task. Analysts must rely on reports from the Ukrainian government, allied governments, cybersecurity companies, and journalists. Yet each of these sources has only partial knowledge of Russian cyber operations, many of which remain hidden. And when operations are discovered, their effects can be difficult to judge, either individually or cumulatively. There is little data, for example, on how Russia's cyber campaigns may have influenced Ukrainian morale—helping either to grind it down or, alternatively, to fuel backlash against the invasion. Moreover, the visible effects of a cyber operation do not always indicate the perpetrator's true intentions. For example, Russia's cyber disruption of a telecommunications network could be a targeted effort to degrade Ukrainian command and control before a key battle. Or it might be part of broader attempts to isolate and immiserate the Ukrainian population. Or it may just be an accidental result of a botched intelligence collection operation.

This paper sidesteps some of these issues by focusing on the actual, rather than intended, effects of Russian cyber operations. It assumes that many undetected Russian cyber operations exist but that they aren't orders of magnitude more effective than known operations. It also looks for indirect evidence of hidden activity. For example, artillery firing patterns might reveal whether or not Russian forces have access to real-time, cyber-derived geolocations of Ukrainian positions. And the paper pairs bottom-up analysis (tactically assessing key Russian cyber operations) with top-down analysis (evaluating the totality of known cyber operations) to discern how cyber activities fit into Moscow's operational plans and overall war effort.

Another challenge is that political or commercial considerations inevitably shape what, when, and how information on Russian cyber operations is shared. The Ukrainian government, for example, has a strategic imperative to offer a relatively upbeat picture of the war so that Western partners continue their support and the Ukrainian people maintain their morale. Kyiv has therefore been reticent to fully disclose casualty figures and other combat losses; the same could be true of cyber incidents.[18] At times, Ukrainian officials have made implausible assertions of cyber success.[19] Meanwhile, Western tech companies have market incentives to portray their own cybersecurity support to Ukraine as highly successful and strategically essential. They may also lack the military expertise to place their findings in context. Microsoft, for example, has been accused of overstating the threat posed by some Russian cyber operations, as well as those operations' significance to military history.[20] Conversely, vendors victimized by Russia (like Viasat) may want to downplay the real-world effects to avoid embarrassment. Western governments and journalists have their own limitations and parochial interests.

This paper attempts to mitigate source bias in several ways. First, it looks for corroboration from multiple independent sources, while highlighting when sources conflict or aren't directly comparable. Second, the paper places more stock in clearcut factual reports (such as descriptions of known intrusions) than in sources' analytic characterizations (like claims that Russian cyber operation are coordinated with kinetic operations). Third, the paper is transparent about sourcing so that readers can draw their own conclusions as appropriate.

Ultimately, a "cyber fog of war" continues to shroud even the most closely watched cyber incidents. A wider fog pervades the war as a whole, which has already undergone several distinct phases in just nine months—often developing in ways that surprise Western analysts (and others). Even so, there is merit in working with the best data and methods available to reduce uncertainty and sharpen understanding. Governments around the world will not wait to incorporate perceived lessons learned into ongoing updates of military cyber strategies, budgets, doctrines, and plans. Analysts should offer the best assessments currently possible while acknowledging information gaps and the need to reassess over time. This paper offers tentative insights representing one reasonable interpretation of fragmentary, conflicting, and evolving data.

Fires

Russia's cyber fires in Ukraine can be categorized in a variety of ways. To understand their military significance, this section groups cyber fires by the type of Ukrainian system targeted—and therefore the potential benefit to Russian forces—rather than by technical characteristics. (Low-level disruptions, such as web defacements and distributed denial-of-service attacks, are generally excluded.) Later, this section evaluates the level of coordination between cyber and kinetic fires and the possibility of cumulative effects.

Against Military Equipment. Moscow's most tangible military need in Ukraine is to suppress and overcome Ukrainian combat power, yet there are no publicly known cases of Russian cyber actors directly disrupting military equipment in the field. Ukraine began the war largely reliant on Soviet-era military equipment, much of which presumably had limited or no connectivity.[21] As the war progressed, Ukraine acquired a large amount of modern, foreign-provided weapons and materiel. The U.S. government has long worried that American military equipment could be subject to wartime cyber attacks by Russia or others. Ukraine now uses some of this same equipment against Russian forces, providing a real-world test of these once theoretical concerns. Yet there has been a near-absence of credible claims that Russia has executed successful cyber fires against Ukrainian military systems. One possible exception: The *Economist* reported in November that unspecified Ukrainian military "networks" and/or "kit" had at some point been "penetrated [and] disrupted."[22] It wasn't clear whether the affected systems were fielded military hardware—such as weapons, vehicles, radios, and intelligence platforms—or merely traditional computer networks operated by the Ukrainian military establishment. Regardless, "the visible effects" were described as "surprisingly limited."

Kyiv and its suppliers and allies might try to suppress evidence of any cyber disruptions of military equipment. According to the *Economist*, Ukraine has done just that. But if strong secrecy can be maintained over a long period, that suggests a smaller number of less consequential incidents. Conversely, Ukraine would probably struggle to conceal a large number of incidents with significant battlefield impact. Electronic warfare (EW) provides a case in point. Russia has sometimes used jamming and direction finding to great effect against Ukraine—for example, degrading Ukraine's drone capabilities.[23] The Ukrainian government may wish to withhold this information, but researchers and journalists have nonetheless documented it extensively. These same sources have failed to note any evidence of disruptive or destructive cyber attacks against Ukrainian military equipment.

Against Communications Networks. Although Ukrainian military hardware has not been directly impacted by any known Russian cyber operations, the communications systems used by Ukraine's military, government, and civilian population have suffered several cyber disruptions. The most notable episode occurred just one hour before the invasion, when hackers working for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation—commonly known as the GRU—perpetrated the so-called Viasat hack. Viasat is a U.S. company that owns a communications satellite called KA-SAT. It provides wholesale satellite broadband services to end users, while an Italy-based company called Skylogic operates and supports the ground infrastructure. According to Viasat, Russian hackers were able to cause "a partial interruption" of Tooway, "a single consumer-oriented partition" of Skylogic's network that provides broadband service to European customers.

Viasat described the hack as "multifaceted and deliberate." The GRU cyber actors first launched a "targeted denial of service attack [that] made it difficult for many modems to remain online."[24] At the same time, they executed "a ground-based network intrusion . . . to gain remote access to the trusted management segment of the KA-SAT network." After moving laterally to reach a sensitive part of the network, the Russians used native software to issue "destructive commands" to "a large number of residential modems simultaneously." These commands "overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable."

The incident had widespread impact, disrupting internet service for "several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe," according to Viasat.[25] Some equipment was quickly restored, while other modems reportedly remained offline more than two weeks later, forcing Viasat to ship tens of thousands of replacements.[26] (Starlink terminals, whose satellite connectivity has for the most part proven resilient, began to arrive in Ukraine four days after the Viasat hack.[27]) Though the bulk of the Viasat disruptions occurred outside Ukraine, Moscow's primary intent was undoubtedly to degrade Ukrainian communications as Russian troops crossed the border and missiles began striking targets throughout the country. Ukraine's military and police were publicly known to be Viasat customers, and Victor Zhora acknowledged that "of course, they were targeting the potential of [the] Ukrainian military forces first."[28] However, the hack's ultimate military impact continues to be debated.

Zhora initially said the Viasat hack caused "a really huge loss in communications in the very beginning of war," which many interpreted to mean military communications specifically.[29] But a spokeswoman for Zhora's agency claimed there was "no information that [the hack] worsened communications within Ukraine's military." Zhora would later specify that Viasat provided only backup connectivity to the military, and that primary landline networks remained online during the invasion; therefore, the hack had no military impact.[30] However, on-the-ground sources have painted a different picture of the state of military communications at the time. Multiple Ukrainian ground commanders who took part in the initial defense of Kyiv have said that Russia "completely jammed the Ukrainians' communications and satellite networks" during the war's opening days and weeks. This effectively grounded Ukrainian UAVs, cut off normal intelligence channels, and left officers "without a link to front-line soldiers."[31]

These reports cited jamming, not hacking, and didn't mention Viasat specifically. But Russia used both methods in concert during its invasion, and they can have complementary effects, which Ukrainian troops may not have distinguished in the heat of battle. Multiple field studies have confirmed that Russia's jamming was quite effective during the assault on Kyiv, at least initially and despite causing some blowback on Russian forces' own communications.[32] Given the apparent fragility of Ukraine's front-line communications links, it seems plausible that the loss of Viasat (whether as a primary communications system or a much-needed backup) contributed to the serious problems cited by Ukrainian commanders. The combination of Moscow's traditional electronic warfare and the Viasat hack seemed to give Russian forces an edge in many early engagements. Russia's ultimate failure to take Kyiv is irrelevant to this analysis; overall strategic failure does not imply that each tactical line of effort, taken on its own terms, added nothing to Russian efforts.

The high-profile nature of the Viasat hack has obscured the fact that another major Ukrainian internet service provider, Triolan, was the victim of a simultaneous cyber attack.[33] Little is known about this event. Triolan was hacked again on March 9, with the attackers reportedly forcing "key nodes of the network" to perform a factory reset. Both incidents led to significant service disruptions lasting perhaps one or two days each. Later in March, the state-owned Ukrtelecom—the country's largest terrestrial telecommunications provider—suffered what it described as "a massive hostile cyberattack" by Russia.[34] Again, details are elusive; Ukrtelecom said that it temporarily "restricted the services for most private users and business customers" in order "to secure the network services for Ukrainian military and critical infrastructure users."[35] The net result of the cyber attack and the remedial measures was an 85 percent loss of connectivity, though service was largely restored by the next day. Kyiv said that military operations were unaffected.

To put these few cyber fires in context, Ukrainians have experienced dozens of significant internet service disruptions due to physical attacks on telecoms equipment and power supplies.[36] Russian cyber fires thus amount to an occasional and secondary threat to Ukrainian connectivity. Overall, Ukraine's telecommunications networks—while somewhat degraded from prewar baselines—have proven remarkably resilient.[37] Key structural factors

include the decentralization of corporate ownership and technical architecture, the agility of engineers, the industry's collaborative wartime spirit, prior investments in cybersecurity, and the availability of supplemental satellite networks like Starlink.[38]

Against Other Computer Networks. Beyond communications networks, Russian cyber fires have targeted a broad range of other government and commercial networks in Ukraine. The most notable incidents have been destructive cyber attacks that delete data and thereby render systems unable to function, which Victor Zhora described as "the most efficient scenario to bring impact to data, to infrastructures, to services."[39] Moscow has carried out an enormous number of these attacks, particularly at the outset of the war. As of late June, Microsoft had detected "eight distinct malware programs—some wipers and some other forms of destructive malware—against 48 different Ukrainian agencies and enterprises."[40] The Ukrainian government reported a similar number: in the first four months of war, fifty-six cyber operations impacted the "availability" of Ukrainian systems (that is, they had destructive or disruptive effects).[41]

Although cyber attacks are difficult to meaningfully quantify and compare in a like-for-like fashion, such figures seem extremely high by any historical standard. For context, the cyber intelligence firm Talos has highlighted just eight important wiper incidents (all state-sponsored) globally from 2012 to 2018.[42] Talos's numbers, although incomplete, are likely the right order of magnitude.[43] This suggests that Russia has performed an unprecedented series of destructive cyber attacks against Ukraine—perhaps the largest series of discrete attacks ever conducted, and possibly more than Moscow had ever carried out, against all targets, in its entire previous history.[44] Citing Russia's attacks on Ukraine, CrowdStrike called 2022 "the most active year yet for wipers."[45]

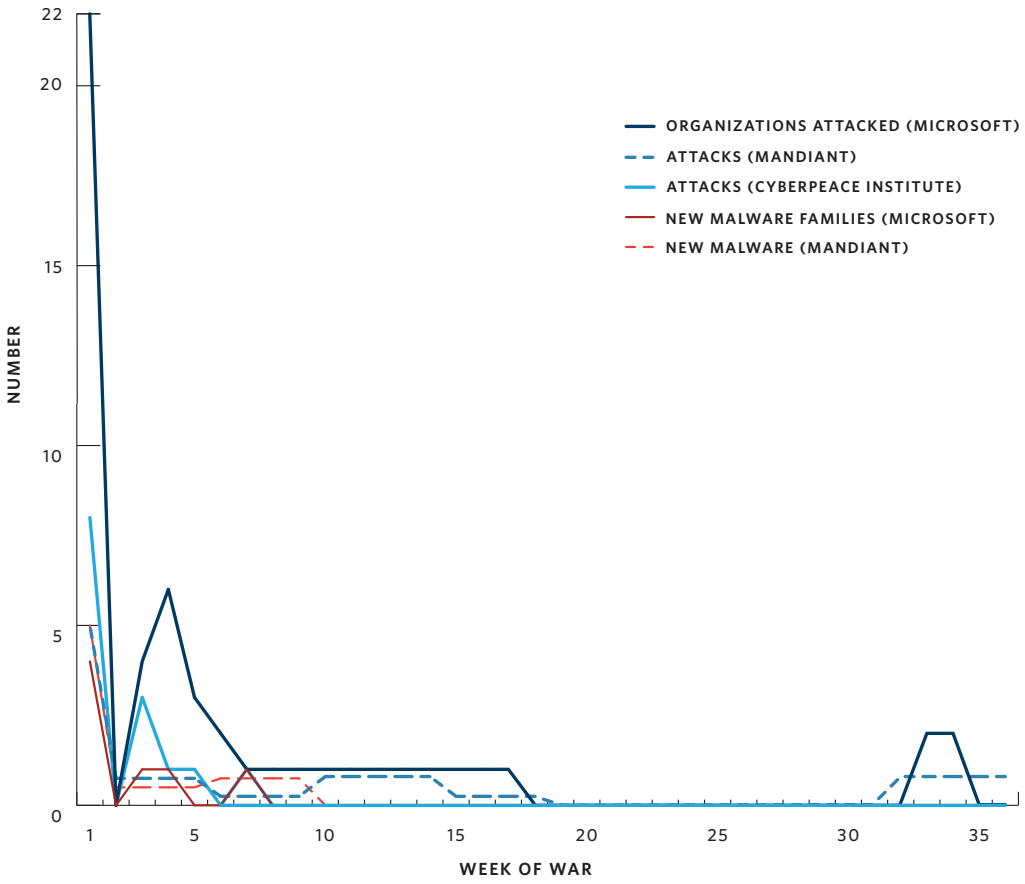
The remarkable scale of Russia's cyber fires in Ukraine is further indicated by the large number of destructive malware variants it deployed. Russia used eight to ten unique families of destructive malware in the first few months of the war, depending on how these are counted.[46] This is a significant portion of all such malware ever known to exist. Lists of wipers compiled by researchers have cited anywhere from six to eighteen noteworthy variants deployed by all actors between 2012 and early 2022.[47] NATO's Cattler and Black noted that, on February 24 alone, Russia "successfully deployed more destructive malware . . . than the rest of the world's cyberpowers combined typically use in a given year."[48]

By all measures, Moscow invested extraordinary effort and technical resources to execute wartime cyber fires against targets such as "Ukrainian government, IT, energy, and financial organizations."[49] However, there is little public information about the impact of these events. Yurii Shchyhol, the director of Ukraine's cybersecurity agency, claimed in July that "none of the cyberattacks that were carried out in the past four months of this invasion has allowed the enemy to destroy any databases or cause any private data leakage."[50] In contrast, Microsoft stated that Russia "permanently destroyed files in hundreds of systems across dozens of organizations in Ukraine," which "at times . . . degraded the functions

of the targeted organizations." Even so, Microsoft said the victims suffered only "limited operational impact." Most of the affected organizations have not been disclosed and there are few public details about how they weathered these incidents.

Moscow's destructive cyber fires in Ukraine were remarkable not only for their total number, but also for their massive concentration at the war's outset and their steep drop-off afterward (see Figure 1).[51] The day before the invasion, hundreds of Ukrainian "systems"—spread across a smaller number of organizations—were targeted, according to Microsoft. Overall, twenty-two organizations faced destructive Russian cyber attacks in the first week of the war. But in the five weeks that followed, Microsoft detected only about three attacks per week on average. By mid-April the figure would drop to just one attack per week, a level that persisted through late June. Microsoft noted "little to no wiper activity" in August and September, followed by a small "spike" in October.

Figure 1: The Rise and Fall of Russian Destructive Cyber Attacks in Ukraine



SOURCE: CyberPeace Institute, Microsoft, and Mandiant. Some data has been averaged or interpolated to enable cross-source comparison, potentially reducing fidelity (see note 51). This chart aims to paint a very general picture of rough patterns and orders of magnitude; it should not be seen as quantitatively precise.

Data from Mandiant and the CyberPeace Institute show broadly similar patterns using different methodologies and information sources. Whereas Microsoft tallied the number of *organizations* attacked, Mandiant has tracked the number of destructive *attacks* (a single attack may affect multiple organizations). Mandiant found five attacks in the war's first week. After that, attacks fell to less than one per week, on average, through October. Notably, Mandiant identified just one attack in the four-month period from June to September, before Russia resumed its destructive attacks in October. The CyberPeace Institute, which compiles public information about cyber operations affecting civilians, also reported a large cluster of destructive attacks in the first few weeks. It documented no attacks from April through October.

This story of destructive cyber fires—a huge surge, rapidly decline, and long plateau—mirrors official accounts. One month into the war, Victor Zhora was already saying that "we do not witness such serious activities as we did at the beginning of the year."[52] In July, Shchyhol described a monthslong "relative lull in the number and quality of cyberattacks of our enemy."[53]

Meanwhile, the number of novel malware variants dropped alongside the number of attacks. Microsoft found that Russia debuted four distinct variants in just the first week of the war, whereas no new variant emerged between early April and late June, the most recent company data. Mandiant likewise saw a spate of new destructive malware in the war's first week, followed by a trickle over the next two months, and then no new malware from May through October. The decline of new malware does not inherently mean a lessening of operational effects. But it is one of several signs that Russian cyber forces faced growing constraints as the war progressed and initial stockpiles of technical resources were expended. Russian hackers have shifted to more quick-and-dirty methods, according to Mandiant, leading to more mistakes.[54] Zhora said in October that Russian cyber attacks had become much less sophisticated since April, devolving into "opportunistic behavior" with "no particular strategy."[55]

The military impact of Russia's individual destructive cyber fires is difficult to judge without victim-level data. Based on the number of attacks alone and Microsoft's high-level characterizations of their results, it is plausible that the early salvo contributed somewhat to Ukraine's initial shock and confusion immediately after the invasion. But within several weeks at most, Russian destructive cyber fires likely receded into the war's background. To be sure, even one state-sponsored data deletion attack per week would be remarkable under peacetime or gray zone circumstances (in any country). But it still seems trivial in the context of a major war. Russian forces have at times launched hundreds of missiles and thousands of artillery rounds per week, inflicting large tangible losses on Ukraine's military forces, civilian population, and infrastructure.[56] There is little reason to think that the dribble of destructive cyber attacks registers on such a scale. To the extent that Ukraine has taken reasonable steps in the face of these attacks—backing up the essential data of critical systems, for example—it is hard to see how Russian cyber fires move Moscow much closer to achieving its military objectives.

Against Industrial Control Systems. Although most Russian cyber fires have targeted digital networks, some have attempted to manipulate or damage physical infrastructure operated by industrial control systems. To date, however, there is no evidence that such efforts have succeeded.

On April 8, the GRU's notorious Unit 74455 sought to disrupt electricity in an unnamed Ukrainian region by deploying malware inside a compromised utility network.[57] This was the culmination of a network intrusion that began in February or possibly earlier.[58] The payload was a more sophisticated adaptation of malware previously used by Unit 74455 in 2016 to interrupt electric power in part of Ukraine.[59] (The unit had done much the same in 2015 using different malware.) Once deployed, the new malware was designed to make service difficult to restore.[60] Zhora said the hackers "planned to cut off 1.5 to 2 million Ukrainians from their power supply."[61] Yet this time, Ukraine's national Computer Emergency Response Team and the Slovakia-headquartered cyber firm ESET detected and stopped the attack in progress.[62] Ukraine initially circulated a document saying the hackers had been able to temporarily turn off nine substations, but Zhora later called this erroneous preliminary information and said that no power disruption occurred.[63] A second failed cyber attack on electric power—discussed in greater detail below—came to light on July 1.[64]

Compared to 2015–2016, Moscow's wartime efforts to disrupt Ukrainian industrial control systems show some technical growth but fewer actual results so far. Meanwhile, Russian kinetic strikes on power infrastructure have caused serious problems throughout the country during the entire length of the war. Periodic electricity blackouts have affected hundreds of thousands to millions of Ukrainians and lasted hours to weeks.[65] The impact on Ukraine's military is unknown, but the civilian suffering has ranged from manageable to severe.[66] On November 4, for example, President Volodymyr Zelenskyy said that 4.5 million Ukrainians had lost power due to a recent spate of Russian kinetic attacks on power supplies.[67]

Coordination of Cyber and Kinetic Fires. Since the outset of the war, analysts have debated whether Russia's cyber fires in Ukraine have been coordinated with kinetic operations to achieve unified military objectives. The strongest evidence is hiding in plain sight: in the twenty-four hours before its invasion, Moscow carried out its most numerous and damaging cyber fires, including the Viasat hack and a massive salvo of destructive operations. These attacks would have required significant preplanning and operational coordination to align with the ground and air assault. But how much did Russia's early scheme of maneuver benefit from this cyber-kinetic coordination? Too little is known about the effects of Russian cyber fires to make a very confident assessment. The Viasat hack, discussed earlier, is the most plausible case of Russian cyber forces contributing to combined arms operations. The hack was near-simultaneous with Russia's first kinetic attacks and may well have aided them—worsening what Kyiv's front-line ground commanders have called a communications-denied environment that impeded Ukrainian defenses around the capital.

It was therefore not outlandish for Dmitri Alperovitch to call the Viasat hack "perhaps the most strategically impactful cyber operation in wartime history," though some qualification and context is needed.[68] Cyber intelligence operations, discussed later, have been part of multiple modern wars and may outstrip cyber fires in strategic importance. For example, U.S. intelligence agencies and military units have used a blend of cyber, signals intelligence (SIGINT), and EW capabilities to geolocate and kill hundreds or thousands of individuals in Iraq, Afghanistan, and elsewhere.[69] If we consider only cyber fires, very few have been

conducted in wartime. The most well-known example is a gray zone incident: in 2007, Israel's cyber-enabled disruption of Syrian air defenses helped Israeli jets destroy a clandestine nuclear site.[70] To cyber skeptics, then, Alperovitch's superlative assessment might be taken as a backhanded compliment—a confirmation that wartime cyber operations (or at least, cyber fires) have only modest value.

Since Russia's initial surge of cyber fires, evidence of cyber-kinetic fires coordination has been more fragmentary, and the handful of proposed cases seem less militarily consequential. The coordination of cyber and kinetic fires could take several forms. To begin with, Microsoft says that "on several occasions the Russian military has coupled its cyberattacks with conventional weapons aimed at the same targets."[71] Microsoft analogized this to "the combination of naval and ground forces long used in an amphibious invasion." Amphibious assaults are highly complex, extended endeavors; a simpler and clearer analogy might be close air support. Just as air assets can be tasked to strike the same tactical targets that ground forces are engaging, so can cyber and kinetic forces.

According to Microsoft, Russia has sometimes used "cyberattacks to disable computer networks at a target before seeking to overrun it with ground troops or aerial or missile attacks." However, the cited examples were inapt. Microsoft highlighted March 2, when it "identified a Russian group moving laterally on [a] nuclear power company's computer network. The next day, the Russian military attacked and occupied the company's largest nuclear power plant." Around the same time, Russia "compromised a government computer network in Vinnytsia and two days later launched eight cruise missiles at the city's airport." But neither of these "cyberattacks" apparently resulted in any disabling effects, precluding them from classification as successful cyber fires. If they were indeed coordinated with physical attacks, they either failed to achieve their intended effects or they were meant as cyber intelligence operations in support of kinetic targeting (discussed later in the paper).

A better example emerged on July 1, with Russian kinetic and cyber fires purportedly aiming at the same target. That day, a Ukrainian power company called DTEK said that Russia had unsuccessfully attempted a cyber attack on the company to "destabilise the technological processes at power generating and distribution companies."[72] The Russian hacker group XakNet, which claims semi-official ties to Moscow, took responsibility.[73] At the same time, Russian forces were carrying out artillery and/or missile attacks on DTEK's Kryvorizka thermal power plant in Kryvyi Rih, Dnipropetrovsk Oblast. DTEK and Victor Zhora both emphasized this connection, with the latter explicitly calling it a case of cyber-kinetic coordination.[74] That is one possibility, but additional context suggests that other interpretations are equally if not more compelling.

The Kryvorizka plant is one of eight thermal power plants that DTEK operates across various regions of Ukraine.[75] DTEK also has numerous other electricity generation, distribution, and related facilities throughout the country.[76] Although Russian troops were clearly firing on Kryvorizka, the cyber attack has not been described as targeting Kryvorizka specifically; it could have been aimed at another DTEK facility or none in particular. Moreover, Russia

reportedly shelled Kryvorizka multiple times in the weeks and months before and after the cyber attack—including on April 27,[77] July 18,[78] and August 2.[79] And at the time of the cyber attack, Russia was launching missile, artillery, and air strikes not only at Kryvorizka but also across Dnipropetrovsk and three neighboring oblasts, among other locations.[80] Russian kinetic attacks on Ukrainian power infrastructure have been a routine feature of the war.[81]

All this suggests the possibility of a spurious correlation between the cyber and kinetic fires on July 1. Indeed, DTEK noted that Russian cyber activities against the company began to "spike" months earlier, in March, following the company's public support for a boycott of Russian energy. DTEK argued that Russia developed a "special focus" on it due to "the firm and proactive position taken by the company's shareholder Rinat Akhmetov with regards to Russia's barbaric war against Ukraine and massive assistance [DTEK] provided to the Ukrainian army and support to Ukrainians."[82] This political motive for the cyber attack, if accurate, would undercut the notion that XakNet's main purpose was to support the tactical aims of Russian troops in the field.

Microsoft acknowledged that it has been "been rare from our perspective" for "computer network attacks" to "immediately precede[] a military attack."[83] It therefore outlined a second, looser category of cyber-kinetic fires integration: threat activity targeting "the same sectors or geographic locations around the same time as kinetic military events." As an example, Microsoft cited a destructive cyber attack by suspected Russian actors "against a major broadcasting company on March 1, the same day that the Russian military announced its intention to destroy 'disinformation' targets in Ukraine and directed a missile strike against a TV tower in Kyiv." While such cases might indicate "active coordinati[on]," Microsoft rightly observed that they could also mean that "computer network operators and physical forces are just independently pursuing a common set of priorities." Regardless, the March 1 case implies some unity of operational objective between cyber and kinetic fires. It raises two further questions: How common is this phenomenon, and how valuable is it for Russian military operations?

The *Economist* reported in November that "American, European and Ukrainian officials all say that there are many examples of Russian cyber-attacks synchronised with physical attacks."[84] However, very few such examples have been publicly described, and many—if not most—are uncompelling. For example, Microsoft argued that Russia's late-October barrage of missile and drone strikes on Ukrainian energy and other civilian infrastructure was "accompanied by [destructive GRU] cyberattacks on the same sectors. . . . The repeated temporal, sectoral, and geographic association of these cyberattacks by Russian military intelligence with corresponding military kinetic attacks indicate a shared set of operational priorities and provides strong circumstantial evidence that the efforts are coordinated."[85] In support, Microsoft cited five cyber incidents: one targeting Ukrainian and Polish transportation and logistics companies, and four targeting other "critical infrastructure." Yet none of these incidents apparently targeted energy infrastructure, which was the primary focus of Russia's October missile barrage. To be sure, it is still notable that Russia in October resumed its destructive cyber fires (after a lengthy quiet period) while also greatly intensifying

its missile and drone strikes. This may reflect some high-level alignment, even if close tactical coordination remains unproven.

The very small number of reported examples suggests that it may not be particularly common for Russian cyber and kinetic fires to strike similar targets at similar times. Although the dearth of examples could reflect information gaps, it seems noteworthy that Microsoft—which has spent hundreds of millions of dollars monitoring and securing Ukrainian networks, and has participated actively in public debates about the war's cyber dimensions—has only catalogued a few suggestive incidents.[86] In addition to these specific incidents, Microsoft has proposed a general geographic correlation between Russian cyber operations and kinetic attacks. Combining proprietary cyber data with third-party information on kinetic activities, Microsoft found that "high concentrations of malicious network activity," though not necessarily fires, "frequently overlapped with high-intensity fighting during the first six-plus weeks of the invasion." However, the correlation was observed at the level of oblast, or province. Ukraine's oblasts average more than 9,000 square miles in size—probably too large to make useful judgments of this kind. Furthermore, the degree of correlation was quite limited. Cyber and kinetic activity matched (that is, "high-high" or "low-low") in fifteen oblasts, whereas it did not match (that is, "high-low" or "low-high") in nine oblasts.

Effectiveness of Integrated Cyber-Kinetic Fires. Russia has probably achieved some unity of purpose with certain cyber and kinetic fires, primarily through loose alignment and more rarely via close coordination. But it is essential to ask, once again, what military benefits this has yielded. The question of military gains must continually be brought back to the foreground in any strategic analysis of Russia's wartime cyber operations.

Consider another case highlighted by Microsoft: an unspecified "Dnipro government agency [was] targeted with [a] destructive implant" on March 11, the same day that the "first direct Russian strikes hit Dnipro government buildings, among others."[87] Further information about the cyber attack is not publicly available, but Ukraine's State Emergency Service announced that three Russian airstrikes that day landed near a preschool and an apartment building and struck a shoe factory (none of these were described as government buildings).[88] One person died. At this stage of the war, Dnipro had been largely spared from Russian attack, despite some unverified earlier reports of limited strikes on noncivilian areas.[89] The simultaneous occurrence of a destructive cyber attack and the first major Russian strikes on the same city is strong evidence of cyber-kinetic fires coordination—perhaps the best candidate since February 24. It could be an example of what Max Smeets has called "pooled interdependence," where cyber and kinetic actions "may not directly depend on each other, [but] each provides individual contributions to the same goal."[90]

The military significance of these coordinated fires must be assessed in the context of Russia's campaign plans. In the preceding days, Russia had been observed massing troops west of nearby Kharkiv, for the likely purpose of "launch[ing] a wide offensive southwest" to "encircle" and assault Dnipro and other cities in the area.[91] Russia may therefore have intended to

stoke fear and panic by striking civilian targets in Dnipro, setting the psychological conditions for its planned siege of the city.

Lacking evidence of the cyber attack's effects, we can explore plausible best-case scenarios for Russia. The cyber attack may perhaps have added to a sense of unease among city officials or residents, especially if it succeeded in deleting data. However, the death and physical destruction caused by the missile strikes would presumably have had far greater psychological impact. Given that the cyber attack targeted a government agency, it could conceivably have hindered local officials' response to the missiles—provided that the affected agency was related to the strike targets, or was involved in emergency services, public communication, or the like. The impact of such a cyber attack would depend on its sophistication as well as the digital and operational resilience of the targeted agency. An extreme best-case scenario for Russian cyber forces would posit that the missile wounded but did not initially kill the Ukrainian victim, and the cyber attack then delayed emergency medical services long enough to cause death. (A direct link between a cyber attack and a fatal delay in medical care has been alleged only twice, globally, and not yet proven.[92]) Speculatively, then, the cyber attack had somewhere between zero and marginal military benefits for Russian operations in the area.

This operational-level assessment can, in turn, be translated to the strategic level by considering the relevance of Dnipro to Moscow's larger war efforts. Although Russia looked poised to attack the city on March 11, it lacked the combat power to actually do so, according to the Institute for the Study of War. The relevant Russian forces were bogged down by "the protracted siege of Mariupol" and faced "the continued ability of Ukrainian forces to carry out successful local counterattacks" near Kharkiv.[93] By the time Russia took Mariupol, it had missed the window to attack Dnipro. Moscow's push into central Ukraine was proving unsustainable and its overall war plan had clearly failed. Within weeks, Russian leaders would finally accept this reality and shift to a near-exclusive focus on eastern Ukraine.[94] In the months since, Dnipro has not again been threatened by Russian troops, though it has faced intermittent missile strikes on civilian and defense-related infrastructure.[95]

Ultimately, then, the March 11 cyber-kinetic fires on Dnipro were largely wasted efforts. This case study shows the complexity of assessing the military impact of cyber-kinetic coordination. Even tactically effective and operationally well-conceived combined-fires actions can only contribute to strategic success if a sensible overall war plan is in place (see Table 1). Granted, a single fires action of any kind can only have so much impact. But this cyber operation was one of just several dozen Russian destructive attacks known to have occurred during the entire war. Within such a small universe of operations, the impact of each one matters in assessing the overall importance of Russian wartime cyber activities.

Table 1. Dnipro Case Study—Speculative Best-Case Russian Benefits From Kinetically Coordinated Cyber Attack on March 11

Tactical	**Modest.** Permanent deletion of data in one local government agency.
Operational	**Marginal.** Delay of emergency response to the missile strikes, contributing to one death.
Strategic	**None.** The cyber-kinetic strikes were intended to support a later ground assault that was militarily unachievable, part of a soon-abandoned war plan, and ultimately never attempted.

Cumulative Impacts. Russia's ability to coordinate cyber and kinetic fires, although important, is not necessarily determinative. Fires can have military effects even when they are poorly or loosely coordinated across weapon systems and domains. For example, Moscow has seized and held a fair amount of Ukrainian territory despite serious, persistent problems in traditional combined arms integration. The Russian way of war is quite imprecise: in Ukraine, Russian forces have generally sought to disrupt and demoralize Ukraine's society, government, and armed forces. Their cruder and more diffuse methods have included random attacks on civilians in Russia-controlled areas, rape as a tool of war, and terroristic missile strikes on civilian areas of cities far from the front lines. Russian tactics have only become more indiscriminate as the war has dragged on. Yet this does not mean they have had no military effect. By the same token, Russia's large-scale cyber fires should be assessed for their possible cumulative impact in Ukraine, notwithstanding their limited coordination with kinetic operations.

Frameworks for assessing the battle damage of individual cyber operations remain immature; understanding cumulative impact is even harder.[96] Still, rough orders of magnitude may be discernible and can have utility for analysts and policymakers. One approach is to loosely compare the total effects of cyber and kinetic fires, based on available quantitative and qualitative metrics. This can be done from two complementary perspectives. Cyber fires can be understood as direct equivalents of kinetic fires, or alternatively, as serving distinctive functions based on their unique features.

Table 2 directly compares some of the total effects of Russian cyber and kinetic fires against similar classes of Ukrainian targets.[97] This exercise has obvious limitations, both empirical and conceptual. Missile strikes are not the same as data deletion attacks, and the various military effects of each haven't been fully documented in Ukraine. More fundamentally, high numbers of attacks, body counts, and damaged targets do not equate to successful warfighting. Even so, it is revealing that, during the first four months of the war, Russia carried out 3,654 missile strikes but only about fifty destructive cyber attacks, according to Ukrainian and Microsoft data.[98] And it is fair to surmise that each missile strike, on average, had greater military benefits for Russia than each destructive cyber attack. One can imagine possible counterexamples—such as a destructive cyber attack that paralyzes Ukrainian rail shipments and thereby delays the delivery of critical supplies to a contested front—but there is no evidence of any (except possibly the Viasat hack).[99] Rather, Microsoft has reported "limited operational impact" from data deletions, whereas missile strikes have destroyed many strategic Ukrainian assets such as military bases, heavy weapons plants, and port, rail, and air infrastructure, in addition to civilian targets.

Table 2. Direct Comparison of Russia's Cyber and Kinetic Fires

Target type	Cyber fires effects	Kinetic and EW fires effects
Weapons systems and materiel	No publicly known cases of cyber disruption to any Ukrainian or foreign-provided weapons systems or other military equipment.	Ukrainian losses of 10,000 troops, 1,300 infantry fighting vehicles, 400 tanks, and 700 artillery systems from kinetic attacks as of June, according to Kyiv.
Military communications	A one-time disruption of thousands of Viasat modems, lasting days to weeks during the initial invasion, plausibly contributing to the partial denial of Ukrainian front-line communications during Russia's assault on Kyiv.	Repeated, intense jamming of satellite and radio communications both during and after the initial invasion, at times seriously degrading Ukraine's military communications and hindering its battlefield performance.
National/civilian communications	5 provider-level telecoms service disruptions, lasting hours to weeks, due to Russian cyber attacks as of May 1. Probably limited disruption to Ukrainian military; manageable civilian suffering.	21 provider-level telecoms service disruptions, lasting hours to weeks, due to Russian kinetic strikes on power and telecoms infrastructure or war-induced financial problems as of May 1. Probably limited disruption to Ukrainian military; manageable civilian suffering.
Electrical power	No known disruptions caused by cyber attacks as of early November. Two known failed attempts.	Periodic blackouts affecting hundreds of thousands to millions of Ukrainians, lasting hours to weeks, due to Russian kinetic strikes on power infrastructure. Unknown impact on Ukrainian military; manageable to severe civilian suffering.
General/other	Roughly 50 Ukrainian organizations affected by destructive cyber attacks as of late June. Limited operational impact.	3,654 missile strikes as of late June, destroying or damaging strategic Ukrainian assets such as military bases; heavy weapons plants; port, rail, and air infrastructure; and civilian targets. 20,000 artillery strikes per day as of July, killing thousands of Ukrainians and causing massive infrastructural damage.

Many analysts resist a direct comparison between cyber "weapons" and their kinetic counterparts. Instead, they emphasize the distinctiveness of cyber operations, such as their ability to achieve reversible, deniable, or systemic effects. The unique features of cyber fires indicate that militaries might sometimes use them in different situations, or for different purposes, than kinetic fires. Table 3 evaluates these features in the context of Russia's cyber activity in Ukraine. It suggests that Russia has not taken advantage of them during the war.[100]

Table 3. Russia Has Not Leveraged the Unique Advantages of Cyber Fires in Ukraine

Unique advantage of cyber fires	Russian results
Limited physical and collateral damage	Russia's initial war plan arguably aimed to limit the amount of permanent, physical, and collateral damage in Ukraine to facilitate eventual occupation. Yet Russian data deletion attacks peaked during this early period, indicating a willingness to cause permanent damage (at least digitally) to Ukrainian organizations. Regardless, what Russian restraint there was did not last long. Once the invasion foundered, Russia began to inflict broad-based suffering, terror, and destruction in Ukraine—both as a means of political pressure and due to lack of military professionalism. To whatever extent Russia has been restraining its cyber fires in Ukraine, continuing to do so would contravene its overall strategy and produce no significant benefits.
Reversible effects	
Deniability	Moscow frequently portrays its war as less brutal than it is and seeks to blame Ukraine for Russian atrocities. Cyber operations might conceivably offer an extra layer of deniability. Under wartime conditions, however, this deniability is even more implausible than usual. Observers have generally assumed that Russia is culpable for all significant cyber operations against Ukraine since the invasion began. More fundamentally, it is Russia's heinous kinetic attacks on civilians that have permanently scarred its international reputation. Deniability of Russian cyber attacks is beside the point when most Ukrainians and much of the world see Putin as a historic war criminal.
Geographic reach	Prior to the 2022 invasion, cyber operations offered Russia a way to act inside Ukraine without physically exposing its personnel and equipment. But once the war began, Russian kinetic attacks—especially missiles—became able to strike anywhere in the country.
Cost-effectiveness and scalability	A cyber operations unit operating inside Russian territory is likely cheaper than a comparably sized combat arms unit that must be forward deployed and supported by a long logistical tail. However, once Russia committed to a large-scale invasion of Ukraine, many of the primary costs of physical deployment became fixed and sunk. To the extent that Russian cyber forces remain relatively cheap, this has not rendered them relatively available for use at scale. Russia has been able to launch thousands of missiles and perhaps millions of artillery shells due to "vast stockpiles" of Soviet-era munitions—and "by some estimates, several years' worth still remains." In contrast, Russia has mustered only dozens of significant known cyber fires.
Systemic effects	Cyber fires can theoretically cause systemic effects if they spread widely, exploit single points of failure, or trigger cascading impacts on a series of interconnected systems. Russia demonstrated this with its 2017 NotPetya destructive attack, which disrupted hundreds of Ukrainian organizations and many others around the world, causing $10 billion in economic losses. However, no similar "wormable" malware has been detected since the invasion, and Russia's known cyber fires have not had any visible cascading effects. In comparison, Russia's kinetic strikes on electric power infrastructure have resulted in failures of water, telecoms, and other basic services, with likely third-order impacts as well.

Conclusion. Overall, cyber fires have not added meaningfully to Russia's kinetic firepower, nor have they performed special functions that kinetic weapons could not. Rather than serving in a niche role, many Russian cyber fires have targeted the same categories of Ukrainian systems also prosecuted by kinetic weapons—such as communications, electricity, and transportation infrastructure. For almost all these target categories, kinetic fires seem to have caused multiple orders of magnitude more damage. Although cyber fires potentially offer unique benefits in certain circumstances, these benefits have not been realized in Russia's war against Ukraine. Moscow's military strategists quickly discarded any aim of reducing physical or collateral damage or creating reversible effects in Ukraine, and Russia has gained little deniability or geographic reach from cyber operations. Likewise, Russian cyber fires have not achieved any systemic effects, and they have arguably been less cost-effective—or at least more capacity-constrained—than kinetic fires.

Intelligence Collection

Compared to their focus on cyber fires, commentators have paid much less attention to whether and how cyber intelligence collection may be supporting the Russian war effort. For example, Lennart Maschmeyer and Myriam Dunn Cavelty argued that Russia has not carried out "cyberwar" in Ukraine, equating this concept with "high-level, destructive cyberattack[s] on civilian critical infrastructures."[101] While acknowledging that "cyber operations . . . remain useful for stealthy intelligence operations," Maschmeyer and Cavelty nevertheless treated intelligence collection as something outside of "cyberwar." Similarly, Chris Krebs wrote that "Moscow's proven cyber capabilities took a back seat in the overall [Russian war] strategy."[102] He based this broad assessment on a narrow look at Russia's disruptive and destructive cyber attacks, without addressing cyber intelligence operations. Likewise, Erica Lonergan, Shawn Lonergan, Brandon Valeriano, and Benjamin Jensen observed in the context of Ukraine that cyber operations "don't win wars, but instead support espionage, deception, subversion and propaganda efforts."[103] This dichotomy omits the fact that espionage during wartime might indeed help one side win.

In fact, intelligence collection accounts for a significant portion, perhaps even a majority, of Moscow's wartime cyber operations in Ukraine. Ukraine's national cybersecurity agency has reported that "enemy hackers" carried out 242 "information gathering" operations during the first four months of the war.[104] By comparison, the agency counted only 56 cyber operations that affected the "availability" of Ukrainian systems (that is, cyber fires). To be sure, cyber operations are difficult to meaningfully quantify and accurately characterize. The same Ukrainian government document counted an even greater number of cyber operations (498) as falling into ambiguous categories—such as "intrusion," "intrusion attempt," or "malicious code"—that do not indicate a clear perpetrator intent or operational outcome. The CyberPeace Institute, which relies on public data and records only cyber incidents impacting civilian systems, gives a lower total number of incidents. Still, it too shows that data thefts (43) were more frequent than destructive cyber attacks (15) from late February through October.[105] (CyberPeace also recorded 103 disruptive cyber attacks during this period—mostly low-level incidents that are easy to carry out and have limited impact.)

These figures are far from definitive, but they match what one might expect. Militaries at war do more than just launch attacks: intelligence remains a crucial task, even after fighting breaks out. U.S. doctrine, for example, defines intelligence as one of seven joint military functions—equivalent in stature to fires. And we know from peacetime and gray zone conditions that cyber operations can be a powerful espionage tool. This may be no less true in wartime. To remedy the lack of attention given to Russian wartime cyber intelligence collection, this section assesses some key ways that such collection might aid Moscow's larger war effort: by providing support to strategic planning, targeting, occupation activities, influence operations, and/or negotiations.

For Strategic Planning. In the lead-up to February 24, the critical military decisions for Moscow were whether, when, and how to attack Ukraine. Putin's process for making these decisions is unclear, but a rational leader would want intelligence assessments of Ukraine's ability and willingness to resist an invasion (among other topics), and Russian security services made significant efforts to meet this need. Ukrainian officials say their intercepts show that, from 2019 to 2021, the Russian Federal Security Service (FSB) unit responsible for Ukraine quintupled in size.[106] Moscow recruited Ukrainian spies not only to provide sensitive information but also to prepare acts of subversion and to facilitate political handover in the event of a Russian invasion. More than 800 Ukrainians—including some senior intelligence officers and opposition politicians—have recently been accused of covertly working for Russia. Moscow supplemented these human intelligence (HUMINT) activities with other kinds of collection. A research firm "with close ties to the FSB" conducted extensive polling in the run-up to the war, "quer[ying] Ukrainians about invasion scenarios in extraordinary detail" to determine how ordinary people would view Russian invaders and whether they would fight back.

Information gleaned from cyber operations was probably also part of Moscow's intelligence picture. Western analysts have long believed that Russia has pervasively penetrated Ukrainian phone networks.[107] In 2014 and 2017, for example, U.S. officials accused Russia of repeatedly recording and leaking sensitive, high-level phone conversations between Washington and Kyiv. Until 2014, most Ukrainian telecoms networks were owned by Russians or Russian-Ukrainians. While this changed after the annexation of Crimea, Moscow's likely former knowledge and access could still be facilitating ongoing intrusions. Russia's cyber espionage, much like its HUMINT activities, grew in the run-up to war. Microsoft reported that "as 2021 progressed, threat actors representing multiple Russian government security services converged on Ukraine to surveil or compromise organizations that could provide valuable intelligence on a Ukrainian military, diplomatic, or humanitarian response to Russian military action."[108] The "target pool" included "Ukrainian defense, defense industrial base, foreign policy, national and local administration, law enforcement, and humanitarian organizations."

It is difficult to judge the utility of Russia's prewar cyber intelligence collection. We lack concrete insight into what information Russian hackers were able to obtain from Ukrainian networks, how analysts in Moscow weighed cyber intelligence against data gathered from other sources, what assessments were ultimately communicated to Putin, and how these

reports might have influenced his final decisions to approve and execute the initial war plan. What we do know is that Moscow grossly underestimated Ukraine's political and military staying power, likely for a multitude of reasons.[109] Russian intelligence agencies have been blamed for their unreliable human sources in Ukraine, their embezzlement of funds, their history of deficits in analytic capability, their poisonous inter-service rivalries, and their lack of candor (both internally and when communicating with Putin). Meanwhile, Putin-watchers have suggested that ideological fervor and poor judgment led him to misinterpret or discount the information available to him. While Kremlinologists debate these factors' relative importance, the overall picture seems clear: deep institutional weaknesses prevented the Russian state from accurately assessing Ukraine's politico-military situation.[110] In such an environment, cyber intelligence collection—no matter how exquisite and voluminous—may have had limited relevance.

For Targeting. Perhaps the most obvious wartime use of cyber intelligence collection is to provide targeting information for kinetic attacks. This can be done in many different ways, two of which are explored below.

First, Russia could use cyber operations to surveil and reconnoiter potential high-value targets for deliberate, precision strikes. Moscow has launched thousands of missiles, air strikes, and precision artillery rounds during the war.[111] Russian stockpiles were large but finite, suggesting the potential value of intelligence in confirming the importance of priority targets and identifying specific aimpoints to cause maximum lasting damage. Although Russian forces have frequently used precision weapons against less significant targets, they have achieved greater impact when attacking strategic Ukrainian assets such as the Yavoriv military base (destroyed by a thirty-missile salvo) and heavy weapons manufacturing plants.[112] Other frequent targets of Russian strikes include port, rail, air, and energy infrastructure, as well as residential and commercial areas (likely targeted to terrorize the populace).[113]

It is inherently hard to observe whether and how Russian cyber intelligence operations are informing deliberate strikes. Still, Microsoft has highlighted two cases where a Russian network intrusion was followed several days later by a Russian missile strike on a seemingly related target. On March 4, assessed GRU cyber actors "compromised a government computer network in Vinnytsia"[114]; two days later, Russia launched eight cruise missiles that damaged military and civilian portions of the Vinnytsia airport, including two control towers and an aircraft.[115] Separately, on April 29, another GRU cyber actor was seen "active[ly operating] within" a "transportation sector network" in Lviv; four days later, Russia missiles struck electrical substations alongside Lviv's railway.[116] In both cases, the timelines make it plausible that Russian cyber actors were feeding intelligence to missile targeteers. However, more detailed information would be needed to support such an assessment and evaluate its significance.

For example, Microsoft has not said whether the compromised Vinnytsia government computer network had any connection to the airport, and if so, whether Russian hackers obtained any data relevant for missile targeting. Assuming they did, the next question would

be whether cyber espionage actually enhanced the missile strikes' effectiveness—that is, by helping to confirm the target's priority and/or refine the aimpoints, and to do this more accurately or rapidly than non-cyber intelligence sources could. By way of example, Russia apparently relied on HUMINT agents to designate certain strike targets in the early hours of the war.[117] But some of these agents provided outdated information that failed to account for last-minute dispersal of aircraft and air defense systems. Had Russian strikes been informed by cyber-enabled communications intercepts or real-time geolocation of key assets and units, Moscow might have had more success in initial operations, such as the crucial airborne assault on Hostomel's Antonov Airport.

From the sparse data available, it isn't obvious that cyber intelligence would have been important for the Vinnytsia or Lviv strikes. Cyber espionage would not be needed to discern the Vinnytsia airport's military importance: its dual-use status was public knowledge, and radar tracks would have confirmed the frequency and patterns of military and civilian flights. Key infrastructure targeted by the missiles—including control towers—was readily identifiable in satellite imagery. The Lviv railway and substations were also in plain sight, though it is conceivable that Russian cyber espionage helped to confirm the railway's logistical importance and its dependence on the targeted substations. (Microsoft assessed that an unrelated GRU cyber operation in Ukraine and Poland "almost certainly collected intelligence on supply routes and logistics operations that could facilitate future attacks."[118]) Even so, the strike's ultimate military impact remains unclear. The day that it happened, a senior U.S. defense official said that "we're still assessing sort of the damage, [but] it's not clear that they've been very accurate in trying to hit that critical infrastructure, and there's been no perishable impact that we've seen to impeding or in any other way obstructing with the Ukrainians' ability to replenish and restore themselves."[119] Microsoft would later state that the Lviv missile strike "disrupt[ed] transport service" in "a key logistical center for the movement of military and humanitarian aid."[120]

In addition to informing the deliberate targeting process for strategic missile and airstrikes, Russian cyber actors might also try to geolocate groupings of Ukrainian forces in real time to support tactical fires such as artillery. The sheer firepower of Russian artillery has been a crucial factor for Moscow, "offsetting" the "generally mediocre performance of Russia's ground forces" for much of the war.[121] Many of Russia's artillery fires have been crude and terroristic: "sustained bombardment," often "overwhelming and indiscriminate," has "levelled [civilian] settlements and infrastructure" in cities such as Kharkiv, Chernihiv, and Mariupol. But well-aimed artillery fires have also been crucial to Russia on the battlefield, "preventing Ukrainian forces from massing to counterattack and causing considerable attrition to those units holding the line. . . . Particularly in Sievierodonetsk, Russian artillery was the key to preventing Ukrainian forces from turning the tables in the close fight as they did in the Battle for Kyiv prior to the Russian withdrawal from that axis." With Russia firing about 20,000 shells per day as of July, granular targeting intelligence (perhaps from cyber operations) could perhaps have substantial effect.[122]

Some believe that Russia already demonstrated such a cyber capability in the pre–2022 Donbas conflict. CrowdStrike has claimed that, from 2014 to 2016, GRU cyber actors tricked Ukrainian soldiers into downloading a malicious version of an artillery targeting app. The infected app was capable of harvesting the victims' "gross locational data," potentially enabling pro-Russian units to "identify the general location of Ukrainian artillery forces and engage them."[123] The malware by itself could not geolocate users with sufficient accuracy to "directly facilitate" counterbattery fire. Rather, the harvested data were said to reveal a rough area for later search by pro-Russian UAVs, which would then "finalize" the targeting process using overhead imagery. The Ukrainian government, the app designer, and some Western cyber analysts disputed CrowdStrike's report—casting doubt on the existence of the compromise, the attribution to Russia, and the claimed battlefield effects. The company largely stood behind its analysis.[124]

So far, no similar reports have emerged since the 2022 invasion, despite Ukrainian forces' even more widespread and effective use of apps for artillery targeting and other purposes.[125] Russian cyber actors might have a variety of ways to try to geolocate Ukrainian units—for example, by compromising cell networks. But field research and interviews in Ukraine have not uncovered any evidence of Russian artillery fire being cued by cyber-enabled geolocation. Rather, a detailed report by Jack Watling and Nick Reynolds found that Russian artillery units use UAV reconnaissance, EW direction finding, acoustic reconnaissance, or counterbattery artillery radar to find Ukrainian positions.[126] Of these, only UAV reconnaissance was able to consistently cue somewhat timely and accurate Russian artillery fire; other mechanisms were more bogged down by "systemic friction and slowed responsiveness" in Russian battlefield communication, coordination, and decisionmaking. This suggests that if Russian cyber actors have somehow geolocated Ukrainian forces without their knowledge, the resulting data must still be confirmed or refined through overhead imagery—much as CrowdStrike had supposed.

Instead of hacking cell phones to acquire real-time geolocation, Russian cyber actors might try to find Ukrainian military equipment by hacking it directly. But there have been no credible, specific reports of this. To counter Ukrainian UAVs, for example, Russia relies on signal jamming or EW direction finding of ground operators, according to Watling and Reynolds; there were no reports of Ukrainians UAVs or their control software being hacked.[127] Many of Ukraine's other combat systems are Soviet-era and pre-digital.[128] Although Western-provided systems could in theory be more vulnerable to cyber intrusions, Russian claims of successful penetrations appear to be bluster. A Russian military expert alleged in August that the U.S.-made HIMARS rocket launcher "has been hacked . . . instantly fixing the launch site."[129] Around the same time, Moscow began claiming successful hits on many HIMARS systems. However, the Pentagon confirmed that all HIMARS were accounted for, and Ukrainian sources said that Russia had launched cruise missiles at wooden decoys.[130] If this is true, the decoys would further confirm Russia's reliance on overhead imagery—not cyber-enabled geolocation—for targeting in the field.

For Occupation. Cyber intelligence collection can be militarily useful even after territory has been seized. Where Russia has controlled parts of Ukraine, its occupation forces must suppress local resistance. In theory, smart occupiers would also seek to restore basic services and administer territory in a way that might build local political support and extract economic value over time. Moscow has focused more on suppression than on rebuilding and administration. Shortly before the invasion, Washington warned the United Nations that "Russian forces are creating lists of identified Ukrainians to be killed or sent to camps following a military operation."[131] This warning did not specify what sources of intelligence Russia was relying on to develop such lists. Open sources would be adequate to identify the most prominent figures hostile to Russian interests, such as politicians, journalists, and intellectuals. Russia's human agents in Ukraine could then help to provide a more textured understanding of the political scene and perhaps identify less prominent likely resisters. (Moscow reportedly recruited at least two possible slates for national leadership of a puppet state, paid numerous collaborators and saboteurs throughout the country, and has found co-optees to run some occupied Ukrainian cities.[132])

Cyber operations could supplement these traditional information sources in several ways. First, mass data collection (such as communication records, geolocation, and metadata) might be used to identify ordinary Ukrainian citizens with links to partisan activity—people without a public record of activism and who aren't personally known to Russia's agents. Cyber activity potentially intended for this purpose has included relentless Russian attempts to penetrate Ukraine's telecommunications companies. Second, targeted cyber espionage could help to verify the political intelligence Moscow receives from its HUMINT sources. The reliability of these sources has been a persistent challenge for Russian intelligence agencies before and during the war. Third, stolen public databases (like address lists and passport information) could facilitate the tracking, arrest, and/or assassination of targeted individuals. For example, shortly before the invasion, Russian cyber actors breached Ukraine's Ministry of Internal Affairs and acquired a national car insurance database, among other relevant data.[133] Granted, similar information might be directly available to Russian occupiers via Ukrainian computer networks and personnel physically under their control. But Ukrainians sometimes wiped key data in advance of Russian territorial gains, putting a greater premium on any information that Russian hackers had already obtained from afar.[134]

Despite the many ways that cyber intelligence collection might be useful to Russian occupiers, Moscow has generally seemed to favor cruder, harsher tactics in its areas of influence. Rather than assembling a careful intelligence picture of local citizenry to facilitate the selective suppression of key resisters while currying favor with others, Russian forces have more often carried out brutal and at times indiscriminate large-scale violence, relied on physical intimidation, and neglected to restore basic services (including internet) in many areas.[135] Russian atrocities in the Kyiv suburbs, particularly Bucha, represent an extreme case of a pattern observed throughout the country: countless instances of arbitrary killings, rapes, looting, and other crimes committed by poorly trained and loosely supervised Russian troops who choose their victims casually or even randomly.[136]

In Mariupol, Russian forces essentially demolished the city before taking over, causing at least three-quarters of the residents to flee.[137] Weeks passed without any serious effort to restore basic services such as electricity, communications, and medical care.[138] Internet and phone service remained very limited one month after the takeover. Even after three months, most citizens still lacked electricity or running water.[139] In the Donbas, Kyiv has said that Moscow deported more than a million Ukrainian citizens to Russia. People who remain have been subjected to "humiliation, torture, robbery—or arbitrary, extrajudicial killing."[140] This roughly tracks with how Russia and its militia allies have governed eastern Ukrainian territory under their control since 2014. Reports from the Donbas depict Russian neglect and chaos, not a sophisticated surveillance state.[141]

The most notable exception was Kherson. Within a few weeks of taking the city, Russian occupiers ordered local Ukrainian officials to reroute internet and mobile traffic through Russian national infrastructure—enabling Moscow to apply its own internet regulations, surveillance, and censorship to Kherson.[142] Citizens could only buy SIM cards with Russian phone numbers and had to display their passports to do so. Russian authorities blocked access to Ukrainian and independent news media, as well as Facebook, Instagram, and Twitter—though not Telegram. The special efforts to control Kherson's internet could stem from the fact that it was "the only provincial Ukrainian capital captured intact by Russian forces" and other cities were simply too decimated to be worth the effort.[143] Kherson's geographic location (near Russian-controlled Crimea), economic value (as a port city), and political status (annexation was planned) may have also played a role. Kherson showed that, under the right circumstances, Russian occupation forces place high value on cyber surveillance. At the same time, it seemed to indicate that physical control of telecommunications networks offers the ultimate cyber collection toolkit for occupiers; next to this, remote hacking would be a more modest capability.

For Influence Activities. The full breadth of Russia's wartime influence, propaganda, and disinformation activities in Ukraine is vast and beyond the scope of this paper. But there are at least two ways that cyber operations can provide direct intelligence or operational support to Russian influence efforts. First, Russian cyber actors can carry out so-called hack-and-leak operations—the digital theft and publication of sensitive data meant to discredit, distract, or demoralize victims. In March, Microsoft observed two different cyber actors—one tied to the GRU, and the other a "suspected Russian threat actor"—compromise "an institution in Ukraine that was featured in false Russian weapons conspiracies in the past."[144] It is unclear whether any sensitive data were exfiltrated or later published. The CyberPeace Institute has documented just five hack-and-leak incidents targeting Ukraine, including three by the self-described Russian hacktivist group XakNet.[145] (By comparison, Russia has suffered sixty-three such incidents during the war.)

Second, Russian cyber actors can use compromised systems or networks as platforms for disseminating influence material. In March, a deepfake video of Zelenskyy calling on Ukrainians to surrender was uploaded to social media.[146] Hackers then gained access to a TV channel, Ukraine 24, to help spread the fictitious story. They placed a still image from

the video on the channel's website, and they edited the chyron text, scrolling below the live TV broadcast, to reflect the deepfake narrative. Despite these efforts, the video was unconvincing and readily debunked.

Later in March, Ukrainian intelligence announced the discovery and remediation of a botnet in the Dnipropetrovsk region that was being remotely controlled by Russia's security services.[147] Moscow had reportedly used the botnet to send about 5,000 propaganda text messages to Ukrainian troops and law enforcement. This number seems small, given that Russia has been sending similar texts since 2014, often using fake cell towers rather than cyber operations.[148] The effectiveness of these messages is unknown. The morale of Ukrainian forces has waxed and waned during the conflict, with some desertions occurring in June.[149] The core problem then was high casualties driven by Russia's artillery overmatch.[150] Propaganda texts would be a marginal factor by comparison, though they could help to cement and aggravate the preexisting concerns of Ukrainian troops and civilians.

From public evidence, it does not seem that Russian cyber actors have made very serious efforts to support influence operations in Ukraine. But undiscovered or undisclosed activities may reveal a different picture.

For Negotiations. Russia and Ukraine conducted several high-level negotiations in late February and March, which did not yield any significant results. There have subsequently been limited, fragile agreements on some humanitarian issues, but no serious proposals for large-scale cease-fires or a negotiated settlement of the war.[151] Still, many observers expect the war will someday end at the bargaining table.[152] At that stage, Moscow could greatly benefit from strategic intelligence on Ukrainian senior leadership—its perceptions, intentions, plans, stances, debates, and schisms. Even now, with no negotiations on the horizon, intelligence on Zelenskyy's inner circle could help Putin and his military chiefs design military operations to maximize political leverage.

The Ukrainian government has detected "a lot of attempts to hack Ukrainian officials' phones, mainly with the spreading of malware," though it claimed in June that none of these attempts were known to be successful.[153] Top leaders have secure devices and networks available for some purposes. Washington gave Zelenskyy a "secure satellite phone" to communicate with the U.S. government, and his office apparently possesses secure landline networks for internal communication with national security agencies.[154] Generally speaking, Ukrainian counterintelligence and operational security efforts have outperformed all reasonable expectations—as demonstrated by the numerous foiled attempts to assassinate Zelenskyy.[155]

Still, Zelenskyy and his inner circle have some inherent cyber vulnerabilities owing to their necessary use of unsecured internet and cell connections. Zelenskyy's masterful social media activity has been crucial in rallying the Ukrainian people to resist Russian aggression and in persuading foreign leaders and societies to provide essential military, humanitarian, and diplomatic aid. Andriy Yermak, head of the presidential office, said that in the early weeks

of the war, "he regularly texted photos of slain Ukrainian children and ruined Ukrainian homes to the cellphones of officials around the world, including Jake Sullivan, the White House national security adviser; Karen Donfried, the assistant secretary of state for European and Eurasian affairs; and members of Congress."[156] Zelenskyy, Yermak, and other close confidants may benefit from software encryption in some contexts. But in general, their use of internet-connected devices—although a strategic imperative—will create continued opportunities for Russian cyber actors to try to collect intelligence. If the Russians succeed in this, the impact on eventual negotiations may manifest in the future and might never be known.

Conclusion. Intelligence collection—not fires—has likely been the main focus of Russia's wartime cyber operations in Ukraine, yet this too has yielded little military benefit (see Table 4).[157] Many of Moscow's military intelligence needs can be fulfilled more readily by non-cyber sources. More fundamentally, Russia's ham-fisted overall approach to the war—from its campaign planning to its occupation of seized territory—suggests that key military decisions are not guided by a rigorous all-source intelligence process.

Table 4. Comparing Russia's Cyber and Non-cyber Military Intelligence Collection in Ukraine

Intelligence support to...	Cyber collection	Non-cyber collection	Limitations on use
Prewar planning	Likely phone surveillance. Attempted cyber intrusions of Ukrainian military, diplomatic, industrial base, administrative, and humanitarian agencies and organizations.	More than 800 alleged HUMINT sources, including some senior intelligence officers and opposition politicians. Extensive polling on invasion scenarios. Open-source information on Ukrainian politics and military readiness.	Pervasive weaknesses in Russian intelligence analysis, internal communication, and decisionmaking, leaving Moscow unable to competently assess the available information on Ukraine's politico-military situation.
Strategic targeting	At least two cases of Russian cyber intrusions plausibly providing intelligence to missile targeteers, but no reason to think this made the strikes more effective.	Satellite and UAV imagery, radar, and open sources can identify many strategic targets, confirm their importance, and reveal key aimpoints. Russia apparently also tasked human agents (who sometimes had outdated information) with designating early strike targets.	Russia's missile targeting calculus is at times haphazard. Missiles are sometimes used against strategic targets but also against minor military targets or seemingly random civilian objects.
Tactical targeting	No indication that Russian cyber forces can provide real-time geolocations of Ukrainian troops or equipment to cue artillery, despite claims that Russia had done this in the Donbas as early as 2014.	UAVs, EW direction finding, acoustic reconnaissance, and radar. Of these, only UAV reconnaissance was able to consistently cue somewhat timely and accurate Russian artillery fire.	Training and command-and-control problems have led to "systemic friction and slowed responsiveness" in Russian battlefield communication, coordination, and decisionmaking, limiting the utility of tactical targeting intelligence.

Intelligence support to...	Cyber collection	Non-cyber collection	Limitations on use
Occupation	Breaches of administrative databases and telecoms might aid in identifying, tracking, and interdicting resisters. Cyber collection can help verify data from human sources or preserve data that Ukrainians wiped in advance of Russian territorial gains.	Open sources can identify prominent figures hostile to Russian interests. Human agents could point to less prominent individuals. Moscow reportedly recruited at least two possible slates for national leadership of a puppet state, paid numerous collaborators and saboteurs throughout the country, and has found co-optees to run some occupied Ukrainian cities.	Rather than assembling a careful intelligence picture of local citizenry to facilitate the selective suppression of key resisters while currying favor with others, Russian forces have more often carried out brutal and at times indiscriminate large-scale violence, relied on physical intimidation, and neglected to restore basic services (including internet) in many areas.
Influence operations	Five documented hack-and-leak incidents as of early November. Elaborate cyber-enabled dissemination of a deepfake was quickly debunked. Botnet sent about 5,000 propaganda text messages to Ukrainian troops and law enforcement.	Large-scale, yearslong, multipronged online and offline influence efforts. Control of media, public information, schools, and sometimes TV, radio, and internet in occupied areas.	Russia's war has led to a surge of Ukrainian nationalism, rendering many influence activities ineffective or counterproductive.
Negotiations	The Ukrainian government has detected "a lot of attempts to hack Ukrainian officials' phones, mainly with the spreading of malware," though it claimed in June that none of these attempts were known to be successful. Zelenskyy and his inner circle have inherent cyber vulnerabilities due to their need to use public internet and phone networks.	Russia leverages open-source information, signals intelligence, and any human agents it retains in elite Ukrainian political circles.	As with the initial war planning, Putin and his top advisers may simply disregard intelligence in their dealings with Kyiv. No significant negotiations have taken place since earlier in the war, so the strategic impact of any relevant cyber intelligence collection remains to be determined.

Despite Moscow's institutional limitations, it might still achieve cyber intelligence breakthroughs as the war progresses. Conceivably, Russian hackers could obtain real-time geolocation data that enable the assassination of Zelenskyy or the timely and accurate targeting of Ukrainian forces, particularly those with high-value Western weapons systems. They might also conduct hack-and-leak operations revealing sensitive war information to the Ukrainian and Western public, such as Ukraine's combat losses, internal schisms, or military doubts; or collect valuable information about Kyiv's perceptions and intentions that can aid Moscow at future talks, among other scenarios. Russian intelligence collection therefore represents the greatest ongoing cyber risk to Ukraine.

Why Have Russian Cyber Operations Not Had Greater Strategic Impact?

Most Western observers agree that Russian cyber operations have not had much strategic impact in Ukraine, but there is less consensus on why. Some cite Russia's cyber incapacity or reticence, while others point to the defensive efforts of Ukraine and its allies. Analysts also vary in whether they focus on the circumstances of this particular war, or on the role of cyberspace in warfare generally. Anne Neuberger, U.S. deputy national security advisor for cyber and emerging technology, acknowledged in July that there are "any number of theories for what we saw, and quite frankly, what we didn't see." She observed that "some argue that we don't quite know" why Russian hackers failed to cause greater disruptions of Ukrainian communications and electric power (for example), and said that "it's certainly something we're watching very closely" in intelligence and cyber policy circles.[158]

Below is a review of twenty-five different factors that have been proposed by Ukrainian and Western officials, companies, and commentators, including some that emerged from this paper's analysis. Building on the observations and arguments made above, each proposed factor is tentatively assigned high, moderate, or low importance as an explanatory factor (summarized in Table 5). This reflects one reasonable interpretation of the evidence.

Individually, these assessments are debatable. Collectively, they reveal that many factors were likely at play. Although some analysts have contended that one or two particular factors were decisive, this appears doubtful. More likely, the reversal of several factors—even one or two with high importance—would not have been enough to significantly improve the overall military utility of Russian cyber operations. In other words, Russia's low cyber success in Ukraine seems to have been overdetermined.

Table 5. Factors Inhibiting Russia's Cyber Success in Ukraine

Assessed Importance	Factor	Category
HIGH	Russian cyber forces were too small to meaningfully contribute to a full-scale war.	Russian Cyber Capability and Capacity
	Russia has been slow to regenerate cyber capability once used.	Russian Cyber Capability and Capacity
	Ukraine's national digital infrastructure was structurally resilient.	Ukrainian Cyber Architecture
	Cloud service providers helped Ukraine migrate key data to secure servers outside of the country.	Foreign Support to Ukraine
	Cybersecurity companies provided advanced end-point security, threat intelligence, and information sharing.	Foreign Support to Ukraine
	Starlink systems bolstered the security and resilience of Ukrainian telecoms.	Foreign Support to Ukraine
MODERATE	Russia's corrupt, incompetent, and ideological national security institutions made cyber intelligence collection less useful for military decisionmaking.	Russian Planning, Organization, and Doctrine
	Russia had across-the-board deficits in combined arms warfare.	Russian Planning, Organization, and Doctrine
	Russian cyber units were organizationally isolated from combat units.	Russian Planning, Organization, and Doctrine
	Russian cyber doctrine emphasized intelligence, subversion, and psychological warfare rather than combat integration.	Russian Planning, Organization, and Doctrine
	Russia chose not to focus its full cyber capacity on Ukraine.	Russian Cyber Capability and Capacity
	Russia's cyber fires had much less psychological and political impact than its kinetic attacks.	Russian Way of War
	Russia's kinetic targeting was too imprecise and haphazard to benefit from cyber-derived intelligence.	Russian Way of War
	Russia's brutal, arbitrary, neglectful, and predatory occupation forces had limited use for cyber intelligence.	Russian Way of War
	Long-term investments in Ukraine's cyber defense ecosystem have paid dividends.	Ukrainian Cyber Defenses
	Ukrainians have used foreign messaging apps that Russia is unable or unwilling to target with cyber attacks.	Foreign Support to Ukraine
LOW	Russia compartmentalized its invasion plans, leaving cyber operators unable to prepare.	Russian Planning, Organization, and Doctrine
	Russia anticipated a rapid military victory that would not require significant cyber operations.	Russian Planning, Organization, and Doctrine
	Russia has been distracted by the need to defend its own networks against foreign cyber operations.	Russian Cyber Capability and Capacity
	Russian forces preserved Ukrainian systems for use in communication or intelligence gathering.	Russian Restraint
	Russian forces preserved Ukrainian infrastructure to facilitate eventual occupation.	Russian Restraint
	Some key Ukrainian systems, such as military equipment, have not yet been digitized or networked.	Ukrainian Cyber Architecture
	Ukraine has had many years of prior experience in monitoring and countering Russian cyber operations.	Ukrainian Cyber Defenses
	Ukraine's "IT Army" has enabled global grassroots cyber professionals to augment Ukrainian personnel.	Ukrainian Cyber Defenses
?·	U.S. and NATO defensive and counter-cyber operations, including "hunt forward," have been effective.	Foreign Support to Ukraine

Russian Planning, Organization, and Doctrine
Russian Cyber Capability and Capacity
Russian Restraint
Russian Way of War
Ukrainian Cyber Architecture
Ukrainian Cyber Defenses
Foreign Support to Ukraine

Russian Planning, Organization, and Doctrine

Factor 1: Russia's corrupt, incompetent, and ideological national security institutions made cyber intelligence collection less useful for military decisionmaking.

Moderate importance. If Moscow had a competent and candid strategic decisionmaking process prior to the war, then cyber intelligence on the state of Ukraine's military and politics might have been valuable in formulating initial Russian war plans, including Putin's crucial decision about whether to invade. We don't know what kind of intelligence Russia's cyber actors obtained prior to the war. And arguably, human and open sources would provide more relevant information on Ukraine's strategic situation—though cyber intelligence can be used to help confirm such information. In any case, we do know that Russia grossly underestimated Ukraine's military and political staying power. This suggests that relevant cyber intelligence, if it did exist, was ignored or discounted by Moscow's intelligence analysts and decisionmakers.

Factor 2: Russia compartmentalized its invasion plans, leaving cyber operators unable to prepare.

AND

Factor 3: Russia anticipated a rapid military victory that would not require significant cyber operations.

Low importance. The quantity and quality of Russian cyber fires actually peaked in the days immediately before and after the invasion, when Moscow launched the Viasat hack and a huge spate of destructive attacks. Russian cyber fires subsequently declined in number, novelty, and impact. If advanced planning were Russia's key limiting factor, one would expect the opposite pattern, as Russian cyber operators would gradually adapt to wartime conditions and began to plan and execute operations in earnest. Indeed, senior Ukrainian cyber official Victor Zhora has so far proved prescient in his April prediction that Russian offensive cyber operations had "likely reached their full potential" and would not "scale" any further.[159] Nine months into the war, there is little reason to suppose that Russia still needs more time to ramp up its cyber operations. While better initial planning could perhaps have made early Russian cyber fires more effective than they were, the overall nature of these operations—which sought to disrupt government and civilian communications and systems on a wide scale—is largely what one would expect based on Russian doctrine and general military principles.

Factor 4: Russia had across-the-board deficits in combined arms warfare.

Moderate importance. Russian forces have struggled in many different ways to synchronize their activities—across warfighting domains, military services, geographic areas, and functional disciplines—and these deficits have significantly hindered Moscow's overall war efforts. When a military has so many serious failures of coordination, including among military roles that have coexisted for decades, the introduction of a newer and less mature capability like cyber inevitably presents enormous coordination challenges. It is likely that better coordination with kinetic forces would have enhanced the military utility of Russian wartime cyber operations. However, the size of this effect isn't clear.

On the one hand, Moscow's cyber operations seemed to have their greatest strategic impact when they were most closely integrated with kinetic operations. The high watermark on both scores came in the first days of the war. That was when Moscow executed its most militarily consequential known cyber operation (the Viasat hack), and its largest spate of destructive cyber operations, to coincide with ground and air operations. On the other hand, Russia's early cyber success depended not only on cyber-kinetic coordination but also on its initially large stockpile of preplanned cyber fires. In the weeks that followed, Moscow's cyber fires declined precipitously as Russian hackers proved unable to maintain such a high operational tempo. Once Russian cyber fires slowed to a trickle (relative to the size of the war), the benefits of coordination with kinetic operations would likewise have fallen. Improving cyber-kinetic coordination probably would not have seemed like a smart priority for Russian theater commanders.

Factor 5: Russian cyber units were organizationally isolated from combat units.

AND

Factor 6: Russian cyber doctrine emphasized intelligence, subversion, and psychological warfare rather than combat integration.

Moderate importance. The GRU has been Russia's lead provider of cyber fires in the Ukraine war.[160] Microsoft stated in December that all "destructive attacks against Ukrainian targets in support of the Russian war effort have been the responsibility of" GRU-associated actors.[161] Although part of the military, the GRU is a national-level element that specializes in intelligence, subversion, and assassination; it is not designed for close integration with regular troops in conditions of large-scale combat. This may help explain why the GRU succeeded in executing a strategic cyber campaign (Viasat and early wipers) to coincide with the initial invasion, but has subsequently failed to show much tactical coordination with Russian units on the ground. However, Russia's cyber intelligence collection operations—presumably a GRU strong point—have not seemed any more impactful than its cyber fires. In particular, public evidence suggests that cyber operations have offered surprisingly feeble support to influence activities, a GRU hobbyhorse. All this suggests that doctrine isn't the whole story.

Russian Cyber Capability and Capacity

Factor 7: Russian cyber forces were too small to meaningfully contribute to a full-scale war.

High importance. To make a serious difference in Moscow's war effort, Russian cyber operations would need to scale to match the size of the war itself. At best, this was achieved only in the war's earliest weeks. Overall, however, Russian cyber operations have barely registered on the grand scale of Moscow's military ambitions and high-intensity combat operations in Ukraine.

To review, Moscow sent more than 150,000 troops to subdue the whole of Ukraine, a country with 44 million people and one of the largest land areas in Europe. Russia launched simultaneous offensives on multiple axes and sent standoff strikes at Ukrainian targets—ultimately thousands of them—in all regions. Eventually, Moscow scaled back its military mission to focus on eastern Ukraine. Even so, the war remained large enough that cyber operations would need to be either incredibly frequent or remarkably effective (or better yet, both at once) to make a measurable difference. Yet Russia's significant known cyber fires have amounted to just a few dozen data deletion operations and two failed industrial control disruptions. Among these, the Viasat hack is the only case where public evidence suggests much plausible military impact. In sum, Moscow's cyber onslaught was unprecedented by peacetime and gray zone standards—but it was small relative to the war in Ukraine.

It is unclear whether Moscow took steps to grow its cyber forces, either before or after the invasion. Russia's large and highly capable cybercrime ecosystem has not visibly participated in the war to the extent many had anticipated. The Russian state has long tolerated and co-opted cyber criminals, leading analysts to expect they would be activated as an auxiliary force during crisis or wartime. Although some purported Russian criminal groups and hacker collectives have targeted Ukraine, and XakNet in particular has carried out several noteworthy operations, much of the criminal activity has been low-level denial of service.[162] Overt activity by major Russian ransomware gangs has largely focused on non-Ukrainian targets.[163] However, Russian criminals may be lending assistance in ways that are difficult to detect.

Factor 8: Russia has been slow to regenerate cyber capability once used.

High importance. If Russian cyber forces had somehow managed to maintain the historic tempo of significant operations seen at the war's outset, they could well have had strategic impacts over time. But Russia suffered a steep drop-off in quantity and quality of cyber fires after the first few weeks of the war. The decline of novel wipers, and related tactical shifts by Russian hackers, suggests a limited stockpile of technical resources.

Factor 9: Russia chose not to focus its full cyber capacity on Ukraine.

Moderate importance. The Russian government refrained from conducting significant destructive or disruptive cyber attacks against Ukraine's Western allies from the outset of the war until October, when the GRU carried out a ransomware attack on logistics and transportation companies—two in Ukraine and one in Poland.[164] Even so, Moscow has continued to carry out large-scale cyber espionage and other network penetrations on a global scale. Russian cyber operations against Western targets have either remained stable or increased since the invasion began, judging from numerous reports by Western governments and cybersecurity firms. While the GRU has taken the lead on Russian cyber operations in Ukraine, Moscow's other cyber-capable agencies (such as the Foreign Intelligence Service, or SVR) have largely focused elsewhere.[165]

Statistics published by Microsoft paint a picture of divided Russian attention. The company reports that "64 percent of Russian threat activity against known targets was directed at [networks operated by] Ukraine-based organizations between late February and June."[166] Granted, this level of concentration is a striking reflection of Russia's new wartime priorities; Victor Zhora has said that Moscow tripled its cyber operations against Ukraine from prewar baselines.[167] But Microsoft's figure also means that more than a third of this type of Russian cyber activity continued to be directed outside of Ukraine. The company separately counted Russian attempts to compromise customer accounts on Microsoft-operated online services like Office 365. Surprisingly, just 2 percent of this activity targeted Ukraine. Although Ukrainians comprise a tiny portion of these services' user base, one might still expect Russian cyber actors to have targeted these Ukrainians with greater intensity.[168]

From Russia's perspective, the wisdom of this cyber resource allocation can be debated. On the one hand, Putin views the Ukraine war as existential, implying it should command all available resources. On the other hand, the war has created a number of new national security challenges for Moscow beyond Ukraine's borders. In addition to supporting combat operations, Russian cyber actors must monitor and suppress domestic dissent, collect intelligence on Kyiv's Western allies and seek to deter them from further intervention, and try to obtain technologies that are now denied to Russia via export controls and sanctions.[169] Regardless of its rationale or merits, Russia's decision to maintain and perhaps even expand its global cyber target list has reduced the cyber capacity available for use in Ukraine.

That said, a different resource allocation might not result in dramatically different outcomes. Even if Russia were to double or triple its existing cyber operations against Ukraine, for example, it might still not be enough to materially impact the war.

Factor 10: Russia has been distracted by the need to defend its own networks against foreign cyber operations.

Low importance. There is a small amount of evidence that Russian offensive cyber actors have turned some of their attention to countering cyber threats against Russia—for example, by seeking to hack the Ukrainian IT Army that is itself hacking Russian networks.[170] In general, however, the overlap between Russian personnel, units, and capabilities that Moscow uses for offensive versus defensive purposes may be limited.

Russian Restraint

Factor 11: Russian forces preserved Ukrainian systems for use in communication or intelligence gathering.

Low importance. Russian cyber fires have targeted Ukrainian telecommunications systems and supporting critical infrastructure at all stages of the war—from the disruptions of Viasat and Ukrtelecom to the repeated attempts to interrupt electrical power. Although Russian forces have indeed relied on Ukrainian infrastructure (such as cell service) to communicate and collect intelligence, they have nevertheless taken no visible action to avoid kinetic strikes on telecommunications networks and supporting infrastructure, which have sustained heavy damage throughout the country and have required continuous repair by Ukrainian workers.[171] Ukrainian data centers and broadcast towers have also been deliberately targeted by Russian precision strikes.[172] All this suggests that—for much of the war, at least—Moscow has had no effective, centralized plan to save Ukrainian communications networks for Russia's own wartime use.

Factor 12: Russian forces preserved Ukrainian infrastructure to facilitate eventual occupation.

Low importance. Russia has deployed brutal mass bombardments and siege tactics in many areas. In some places that have been controlled by Russia, such as Mariupol, there were minimal efforts to restore basic services such as electricity, communications, and medical care. This suggests that Moscow has been unconcerned with preserving Ukrainian infrastructure—at least in much of the country—for its eventual control.

Russia may have initially planned for cyber restraint before changing its mind as the war evolved. If so, one would expect Russian cyber fires on Ukrainian critical infrastructure to increase in number and severity over time. Yet Russian cyber fires generally peaked in the days and weeks surrounding the immediate invasion, implying that capacity rather than intent has been the primary constraint. A possible counterexample is Russia's cyber fires on industrial control systems, which did not occur until April and July. Preparation for the July attack apparently began no later than February, suggesting that Russia sought, at a minimum, to develop options for industrial control system attacks as soon as the war began.

Russian Way of War

Factor 13: Russia's cyber fires had much less psychological and political impact than its kinetic attacks.

Moderate importance. Russian forces have killed tens of thousands of Ukrainians, brutalized and terrorized civilian populations, destroyed large portions of major cities, and displaced millions. It is difficult to imagine any cyber campaign—no matter how well-constructed and persistent—that would meaningfully add to this societal and psychological trauma. Nevertheless, we know little about the dynamics of Ukrainian wartime politics and morale. Conceivably, popular Ukrainian support for continuing to prosecute the war has depended in part on Ukrainians' initial and continued ability to hear from their leaders, access basic services, and communicate with family members. If so, a highly effective and sustained campaign of cyber disruptions by Moscow could perhaps have helped force Kyiv to the bargaining table over time. More study of these questions is warranted.

Factor 14: Russia's kinetic targeting was too imprecise and haphazard to benefit from cyber-derived intelligence.

Moderate importance. Russian artillery fires have usually "lack[ed] much of the C4ISTAR [command, control, communications, computers, information/intelligence, surveillance, targeting acquisition, and reconnaissance] coordination as envisioned by the Reconnaissance Fire Complex and exhibit[ed] a considerable degree of systemic friction and slowed responsiveness," according to Jack Watling and Nick Reynolds.[173] In the face of these deficits, Russian artillery units have at times sought to overwhelm their enemy with sheer quantity. It is therefore unclear whether cyber-derived tactical targeting intelligence—for example, precise real-time geolocation of Ukrainian positions—could be productively used by Russian forces. It does seem that some intelligence sources are more successful than others. When Russians can spot Ukrainians via UAV imagery, they have directed artillery fire much more rapidly and accurately than when EW direction finding, acoustic reconnaissance, or radar was used.

Russia's missile targeting process is also variable. Russia has often launched missiles against minor military targets and more or less random civilian objects.[174] In those cases, cyber-derived intelligence would not be of much use. But missiles have sometimes struck strategic targets, such as bases, airports, defense production facilities, transportation nodes, and energy infrastructure. It is conceivable that cyber intelligence collection might have sometimes provided unique targeting information—for example, revealing a hidden dependency or vulnerability. There are a few known cases where Russian cyber operators plausibly fed intelligence to missile targeteers, but it's not obvious in those cases that cyber intelligence was important. Missile targeteers would already know of most strategic Ukrainian targets via traditional intelligence sources. Cyber intelligence would typically be a convoluted and time-intensive way of confirming a target's importance and identifying aimpoints compared to, say, satellite imagery.

Factor 15: Russia's brutal, arbitrary, neglectful, and predatory occupation forces had limited use for cyber intelligence.

Moderate importance. Although available information is sparse, Russian forces in occupied territory do not seem to have used sophisticated intelligence techniques to separate key resisters from other citizens. Rather, they have more often carried out brutal and at times indiscriminate large-scale violence, relied on physical intimidation, and neglected to restore basic services (including internet) in many areas.[175] The most notable exception is Moscow's move in early May to reroute internet traffic from Kherson—which Putin planned to annex—through Russian national infrastructure, enabling Moscow to apply its own internet regulations, surveillance, and censorship to the city.[176] However, this incident serves to highlight that physical control of telecommunications networks can enable far more systemic surveillance than remote hacking.

Ukrainian Cyber Architecture

Factor 16: Ukraine's national digital infrastructure was structurally resilient.

High importance. Ukraine's national internet and IT infrastructure, even before the war, was resilient in many ways. Researchers have identified "low market concentration at multiple levels and the relatively high number of interconnect facilities," meaning "there are no obvious choke points, or individual networks whose loss would have a crippling effect on the internet in Ukraine."[177] Moreover, the country has a thriving workforce of IT professionals and network engineers, and this human element has proven agile, collaborative, and highly motivated to maintain digital connectivity in the face of kinetic and cyber fires.[178]

Factor 17: Some key Ukrainian systems, such as military equipment, have not yet been digitized or networked.

Low importance. There have been no reported hacks of Soviet-era Ukrainian military equipment, much of which presumably has limited or no connectivity.[179] But equally, there have been no credible and specific reports that Ukraine's modern, networked equipment has been hacked. For example, Ukraine's drone operations have proven vulnerable to Russian jamming and EW direction finding, but field researchers have not noted any evidence of hacking.[180] Of course, Kyiv and its suppliers and allies may choose not to publicize any successful Russian hacking of military hardware. However, it would probably be difficult to conceal a large number of incidents with significant battlefield consequences, as demonstrated by Ukraine's well-documented struggles against Russian EW during some parts of the war.

Ukrainian Cyber Defenses

Factor 18: Long-term investments in Ukraine's cyber defense ecosystem have paid dividends.

Moderate importance. Since roughly 2017, the United States has expanded multiple initiatives to bolster the cybersecurity of Ukraine's government and critical infrastructure.[181] In addition, "numerous [other] foreign governments and cybersecurity companies had invested in Ukrainian cyber capacity building over several years."[182] Ukrainian institutions made parallel investments of their own.[183] For example, one of Ukraine's largest telecoms companies grew its cybersecurity workforce by about two-thirds from 2015 to 2022.[184] Such investments may well have contributed to Ukraine's wartime cyber defenses. It is suggestive to compare the periods before and after these reforms. From 2015 to 2017, Ukraine was the victim of three exceptionally damaging Russian cyber attacks: two electrical power disruptions and the NotPetya attack. But from 2018 until Russia's 2022 invasion there were no comparably serious events, despite the ongoing Donbas conflict and occupation of Crimea. Plausibly, the broad-based and sustained investments in Ukrainian cybersecurity led to major improvements in the country's cyber posture.

Factor 19: Ukraine has had many years of prior experience in monitoring and countering Russian cyber operations.

Low importance. If persistent cyber targeting of one country by another leads defenders to develop relative advantages over time, then this pattern would be evident around the world: major state-sponsored cyber actors would show gradually declining efficacy against their primary targets. This does not seem to be the case.

Factor 20: Ukraine's "IT Army" has enabled global grassroots cyber professionals to augment Ukrainian personnel.

Low importance. Although the IT Army was originally announced as having both defensive and offensive missions, research suggests it soon became purely offensive in nature.[185] Any defensive benefits for Ukraine would be indirect, insofar as the IT Army's hacking of Russian systems caused Moscow to retask its own offensive units toward more defensively oriented missions.[186]

Foreign Support to Ukraine

Factor 21: Cloud service providers helped Ukraine migrate key data to secure servers outside of the country.

High importance. Ukraine undertook an emergency cloud migration immediately after the Russian invasion, which Ukrainian government agencies and Western companies have called critical to the country's cybersecurity and digital resilience.[187] Ukraine's digital minister, for example, said that the Amazon Web Services (AWS) cloud platform "literally saved our digital infrastructure."[188] The need for this migration was demonstrated when Russia reportedly damaged a Ukrainian government data center with a cruise missile attack "in the early days of the war."[189] Kyiv said that "no data was lost because backups were available," though it is unclear if cloud migration was the reason; Ukraine's governmental cloud migration may not yet have begun in earnest at that time. In any case, cloud migration has produced wide-scale improvement in Ukraine's overall cybersecurity and resilience.

The migration process unfolded iteratively over several months—with economically critical databases receiving first priority—and remained ongoing as of late July.[190] While this gradual timeline is to be expected for such an enormous and complex undertaking, it also suggests that cloud migration cannot wholly explain Ukraine's successful cyber defenses, particularly in the war's earlier stages. In fact, a cloud migration process can itself introduce various distractions, service disruptions, and new cybersecurity vulnerabilities (such as in the configuration and access interfaces of cloud assets), especially under the strained and chaotic circumstances of wartime. Cloud migration has certainly enhanced Ukraine's wartime cybersecurity, but it is probably not the single decisive factor.

Factor 22: Cybersecurity companies provided advanced end-point security, threat intelligence, and information sharing.

High importance. Microsoft has argued that recent innovations in end-point security, threat intelligence, and information sharing have been some of the most important factors in Ukrainian cyber defenses.[191] For example, the company has declared that "for the first time in a major cyber event, behavioral detections leveraging machine learning used known attack patterns to successfully identify and stop further attacks without prior knowledge of the underlying malware—even before humans were aware of the threats."[192] Other companies, like AWS, have also provided close cybersecurity support to Ukraine, while threat intelligence from Western firms and governments has helped to expose and mitigate malicious activity.[193]

The impact of these efforts is difficult to judge, but their sheer scale is hard to discount. Few if any other moments have galvanized so many of the world's leading cybersecurity actors to protect a single set of victims from a defined set of bad actors. (The 2020 U.S. presidential

election may be the only comparable example.) This extraordinary concentration of cybersecurity capability presents major obstacles for even a determined and powerful adversary like Russia. That said, considerable effort and skill would be required to properly coordinate and leverage the cybersecurity support that Ukraine has received. More information is needed to understand how well Ukraine has done this under trying wartime circumstances.

Factor 23: Starlink systems bolstered the security and resilience of Ukrainian telecoms.

High importance. Ukraine's top cybersecurity official, Yurii Shchyhol, cited Starlink as the most useful form of digital assistance that Ukraine has received during the war.[194] Starlink has reportedly made numerous tangible contributions to the war effort, such as enabling the control of Ukrainian drones, helping besieged Ukrainian troops in Mariupol stay in touch with their commanders, and facilitating Zelenskyy's communications with world leaders and the global public.[195] Starlink's architecture has been relatively resistant to cyber attacks and jamming, though Elon Musk claimed in May that the Russians were "ramping up their efforts."[196]

To be sure, Starlink is not the mainstay of Ukraine's internet. Ukrainian terrestrial telecommunications networks, which have higher bandwidth, have proven fairly resilient during the war, and Starlink users are advised to limit their reliance on the network because its signals pose a risk of discovery and targeting by Russian forces.[197] In early May, Ukraine's digital minister said that "about 150,000 Ukrainians use Starlink on a daily basis"—less than 1 percent of the country's population.[198] But some users are more important to Ukraine's war effort than others. Anecdotally, front-line Ukrainian forces seem to be among the heaviest Starlink users. They often cite Starlink as their most important channel for command and control, and they have described outages as leading to "'catastrophic' loss of communications" on the battlefield.[199] Further research could investigate the extent to which essential communications, such as government, military, and critical infrastructure data, flow over Starlink and Ukraine's various other telecommunications systems.

Factor 24: Ukrainians have used foreign messaging apps that Russia is unable or unwilling to target with cyber attacks.

Moderate importance. Messaging and other communication apps—such as Signal, Telegram, Twitter, and Zello—were widely used in Ukraine before Russia's invasion, making them familiar and valuable channels once the war began.[200] They have long been embraced by Ukraine's government and media, becoming central sources of information about politics and daily life. Russia has used these same platforms to propagandize to the Ukrainian populace. Still, Ukraine's continued access to familiar sources of instantaneous communication has brought more benefits than risks to the country. For example, social media has been an important means for Zelenskyy to reassure his people, particularly in the war's early days when maintaining morale was most essential. More research is needed to understand the many effects of these platforms on the war's progression.

Factor 25: U.S. and NATO defensive and counter-cyber operations, including "hunt forward," have been effective.

Unknown importance. Shchyhol has described "a constant synergy" between his government, U.S. Cyber Command, and the National Security Agency (NSA) to secure Ukrainian networks, "especially of government institutions and military-related installations."[201] But there is no public information about the nature and extent of these activities or their impact.

Conclusion

In sum, many factors have constrained Moscow's cyber effectiveness in Ukraine. Perhaps the most important are inadequate Russian cyber capacity, weaknesses in Russia's non-cyber institutions, and exceptional defensive efforts by Ukraine and its partners. To meaningfully influence a war of this scale, cyber operations must be conducted at a tempo that Russia apparently could sustain for only weeks at most. Moscow worsened its capacity problem by choosing to maintain or even increase its global cyber activity against non-Ukrainian targets, and by not fully leveraging cyber criminals as an auxiliary force against Ukraine. Meanwhile, Putin and his military seem unwilling or unable to plan and wage war in the precise, intelligence-driven manner that is optimal for cyber operations. Ukraine, for its part, has benefited from a resilient digital ecosystem, years of prior cybersecurity investments, and an unprecedented surge of cyber support from the world's most capable companies and governments.

What Lessons Apply to Other States' Military Cyber Efforts?

The Russian war in Ukraine offers some general lessons for other states' military cyber efforts. However, it is crucial that countries consider a range of relevant case studies and account for their own national circumstances, including the specific kinds of wars they might need to fight in the future. Below are some high-level insights and recommendations, with particular focus on the United States and Taiwan.

Cyber Offense

Fires. Russia's experience suggests that cyber fires can be usefully concentrated in a surprise attack or other major salvo, but they risk fading in relevance during larger, longer wars. Cyber commands that hope to sustain fires at militarily relevant levels throughout a

large-scale war should be appropriately sized and designed for this daunting task. What that means in practice isn't clear. At a minimum, Russia's apparent failure to mass adequate cyber force in Ukraine should prompt other countries to reexamine the assumptions behind their own sizing constructs. U.S. Cyber Command, for example, is still sized to its original 2012 model: about 6,200 personnel split into 133 teams, including twenty-seven Cyber Combat Mission Teams that would have primary responsibility for wartime cyber fires (among other tasks).[202] The command plans to add fourteen more teams in the next few years, with two new Combat Mission Teams included among the first additions.[203] U.S. Cyber Command is extremely large by global standards. Even so, it isn't clear that the organization can produce enough cyber fires capacity to meet expectations or needs in a major conflict, notwithstanding modest future growth. The command has said that new teams are being added in response to "recent demand across DoD"—presumably, peacetime and gray zone requirements.[204] Wartime needs would most likely be many times larger.

Militaries that prioritize wartime cyber fires may therefore face a difficult choice. They can opt to maintain huge standing cyber forces at significant expense. Alternatively, they can develop surge capacity mechanisms (drawing on reserves or civilians, for example), which are challenging to implement and risk cannibalizing domestic cybersecurity in a crisis. Moreover, adequate force size is necessary but insufficient to deliver meaningful wartime cyber fires.

The Russian example has also demonstrated the need for rapid regeneration of cyber capabilities. U.S. Cyber Command, too, has sometimes struggled with force regeneration—even under peacetime and gray zone conditions—and has therefore sought to develop lower-cost, "burnable" tools and infrastructure.[205] Such challenges would likely be far more acute in a major war. To make the most out of limited wartime cyber capacity, militaries may need to experiment with wave tactics: short bursts of intense cyber fires followed by periods of stand-down and regeneration. Russia possibly employed this approach when it halted destructive cyber attacks in the summer before resuming in October, around the same time that Moscow intensified its missile attacks. The more infrequent the waves of cyber fires, the more important it will be for militaries to coordinate them closely with kinetic fires.

Russia's war in Ukraine illustrates the high bar of delivering cyber fires at the scale and pace of major conflict. Militaries designed for large-scale war should carefully consider whether meeting this bar is a realistic goal. If their cyber commands cannot scale dramatically and regenerate rapidly, they should perhaps not focus on developing wartime fires in the zone of conflict. They might instead prioritize non-fires activities such as cyber defense operations or intelligence collection. Or they could plan for more selective war-related fires in other theaters, as Russia has done by holding NATO countries' networks at risk in an effort to deter further support for Ukraine. Militaries might also de-emphasize wartime missions entirely and invest instead in peacetime, gray zone, or prewar fires—including what the U.S. military calls "campaigning" or "shaping" operations.

In fact, many countries may already be heading down these various alternative paths. Max Smeets has found that, although more than forty states have established military cyber commands, just a few have ever conducted any known cyber effects operations (fires), in war or otherwise.[206] In this global context, the U.S. military—plus a handful of its friends and rivals—appears to have exceptionally ambitious cyber goals. Most countries should probably not emulate U.S. Cyber Command's bold aspiration to "deliver strategic and operational advantages for the Joint Force . . . in conflict" by "integrat[ing] cyberspace capabilities and forces into plans and operations across all domains."[207]

Intelligence. Cyber intelligence collection may have greater overall potential than cyber fires to support a variety of wartime military tasks. The Russian case, however, shows that realizing this potential requires competent analysis and decisionmaking processes and a reasonably precise "way of war." Russian cyber operators may well have acquired more raw data in Ukraine than could be reliably interpreted and practically used by Russian political leaders, intelligence analysts, planners, targeteers, or occupying forces. As cyber capabilities proliferate, more countries could face this mismatch. In such cases, broad institutional reforms—upgrading analytic tradecraft, instilling professionalism, or combating corruption—will often have more value than further technical investments in cyber collection. Militaries unable to implement those reforms may find that exquisite cyber intelligence capabilities aren't worth the effort to develop.

In addition, cyber operations have specific strengths and weaknesses as a source of wartime intelligence; they are not the right tool for every task. Although cyber operations can yield unique intelligence data, they're more time-consuming and inconsistent than many other methods. Overhead imagery, for example, has most likely been far more important to Russian kinetic targeteers than cyber-derived intelligence. Cyber units should be fully integrated into all-source intelligence processes that direct them toward information needs which cannot be readily fulfilled by other means. Wartime use cases for cyber intelligence might include tracking high-value targets in real time, validating HUMINT in mission-critical situations, and acquiring very large data caches with durable, multipurpose value.

Cyber Defense

Cyber defenders also have much to learn from the Russia-Ukraine war. Their first task is to revisit assessments of enemy offensive cyber capabilities in light of Russian challenges and limitations in Ukraine. Although some of Moscow's struggles may be circumstantial, others could apply more broadly. Cyber defenders should therefore consider whether they have overestimated their respective enemies' likely ability to use cyber operations to win a future war against them. For example, U.S. officials have long worried that an adversary could exploit or disrupt American weapon systems during war, and have therefore worked for years to bolster the cybersecurity of U.S. military hardware. The Government Accountability Office has called for a redoubling of these efforts due to continuing institutional gaps.[208] Yet Russian forces, facing many of the same U.S. systems on the Ukrainian battlefield, have seemingly

failed to compromise them in significant ways. Washington should carefully review its intelligence, and press Kyiv for help, to validate its prior assumptions of how adversaries will use cyber operations against U.S. systems in combat. Realistic assessments help to avoid overinvestment in less important areas, freeing up scarce resources for higher priorities. Cyber policymakers must differentiate between possible worst-case scenarios (positing extreme danger) and more likely cyber events (which may not cause lasting strategic damage).

Taiwan. Different countries should draw different cyber lessons from the Russia-Ukraine war based on their particular military situations. Taiwan, for example, might use Ukraine's experience to better anticipate and defend against Chinese cyber operations during a potential full-scale invasion. Taiwan's plans should, of course, be rooted firmly in its own context. This means carefully analyzing China's cyber and kinetic forces, Taiwanese network architecture and security, possible third-party contributions, and the political goals likely to shape each actor's cyber and overall military strategy. But these factors are not easy to judge, leading to some inevitable reliance on assumptions. The war in Ukraine offers a useful reference point for examining and refining these assumptions. Taiwanese cyber analysts and planners should make comparisons, as well as contrasts, between the Russia-Ukraine war and a possible China-Taiwan war.

To begin with, Russia's inept military and political institutions have demonstrated that effective wartime cyber operations depend on sound decisionmaking and coordination processes. It is noteworthy, then, that Chinese President Xi Jinping has gradually eliminated rival factions and eroded meritocracy at the top levels of Chinese leadership. Are Xi and his yes-men likely to repeat Putin's mistake of failing to rely on objective intelligence—including cyber intelligence—to inform military plans? Or have Xi's efforts to professionalize the military and improve joint warfighting prepared China to make better use of cyber operations?

Russian cyber capacity constraints also invite a reexamination of China's posture. On the one hand, Beijing probably possesses a larger military cyber force than Moscow.[209] On the other hand, China has very rarely attempted any cyber fires, whereas Russia had already carried out many previous destructive attacks. Would China execute an even bigger and more effective cyber salvo at the outset of a Taiwan invasion, or would it bungle the opener due to inexperience? And what happens after that? Many observers expect a Chinese invasion to lead to a protracted military struggle. Would Chinese cyber forces demonstrate greater regenerative capacity than Russia, or would they likewise become less militarily relevant over time?

Finally, Taiwan's cyber architecture and defenses should be considered in light of the Ukrainian experience. Taiwan has greater technical prowess than Ukraine, so would its military and civilian communications infrastructure prove even more resilient? Or does Taiwan's island geography mean fewer, more vulnerable choke points—with the risks potentially magnified by a higher overall dependence on digital technology? International cyber

assistance, so critical to Ukraine, may be Taiwan's biggest question mark. Western technology companies have had powerful political, reputational, and commercial motivations to support Ukraine.[210] But unlike Ukraine, Taiwan lacks a clearcut claim of sovereignty. And compared to Russia, China has much greater economic heft and global technological integration. Would Western companies be just as eager to help Taiwan? If so, would they be physically able to do so without overland access?

Posing these questions is easier than answering them. But they suggest some ways that other countries can look for cyber lessons in the Russia-Ukraine war without losing sight of their own distinct circumstances.

Conclusion

Russia's cyber operations in Ukraine have apparently not had much military impact. This was probably for a multitude of reasons: Russia's offensive limitations, as well as the defensive efforts of Ukraine and its partners; the particular context of this war, as well as structural features of cyberspace and warfare generally. The Russia-Ukraine war offers an important case study of cyber operations as a wartime military instrument. Yet it is neither the first nor the only such case study. Other militaries have previously used cyber operations, in war or combat situations, with varied outcomes. Militaries with high capability, professionalism, and readiness in both cyber and kinetic disciplines—such as the United States and Israel—have leveraged cyber intelligence collection and fires to enable strikes on high-value targets, for example.

But even top-tier militaries seem to have the greatest cyber successes in tightly circumscribed contexts. Former U.S. secretary of defense Ashton Carter, for example, wrote that he was "largely disappointed in Cyber Command's effectiveness against [the self-proclaimed Islamic State]"—arguably the largest and most intense U.S. military campaign since the maturation of American offensive cyber capabilities. According to Carter, U.S. Cyber Command "never really produced any effective cyber weapons or techniques" in the campaign.[211]

Russia's invasion of Ukraine is an even larger and more ambitious military endeavor than the U.S. campaign against the Islamic State, and it seems to reaffirm an emerging truth of wartime cyber operations: modern wars will always feature cyber operations, but cyber operations won't always be important to these wars. Rather, the scale of war appears inversely correlated with the strategic impact of cyber operations. If this correlation holds, cyberspace should probably not be seen as a "fifth domain" of warfare equivalent in stature to land, sea, air, and space.[212]

About the Author

Jon Bateman is a senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace.

Acknowledgments

The author is very grateful to Dave Aitel, Nick Beecroft, Steven Feldstein, Ariel (Eli) Levite, Arthur Nelson, George Perkovich, Max Smeets, and Gavin Wilde for their valuable feedback on versions of this paper, and to many other experts and officials who shared relevant insights and critiques while the paper was under development. The author would also like to thank June Lee and Gerald Torres for research assistance. The final paper reflects the views of the author alone.

Notes

1 For the purposes of this paper, "cyber operations" refers to the hacking of computers and digital systems, primarily by remote means (over the internet) but also when facilitated by human agents. Related concepts—namely electronic warfare, signals intelligence, and influence operations—are not a primary focus. While these related ideas are intertwined with cyber operations in Russian doctrine and can be blended, this paper cannot consider them all in depth. The paper primarily focuses on cyber operations directed or orchestrated by the Russian state—whether ultimately carried out by military members, intelligence officers, criminals, or others. It does not consider truly independent pro-Russian hacktivism (to the extent such a thing exists). Nor does it evaluate Russian cyber operations conducted against non-Ukrainian targets, though many of these (such as intelligence gathering and operational preparation in NATO country networks, or online suppression of Russia's own citizens) are connected to the war. Finally, offensive cyber operations by pro-Ukraine actors, including the United States and NATO, are also beyond the scope of this paper.

2 The word "cyber" is never used in the following major narratives of the war and its key battles: "Ukraine Conflict Updates," Institute for the Study of War, accessed November 15, 2022, https://www.understandingwar.org/backgrounder/ukraine-conflict-updates; Andrew S. Bowen, "Russia's War in Ukraine: Military and Intelligence Aspects," Congressional Research Service, September 14, 2022, https://crsreports.congress.gov/product/pdf/R/R47068; and Paul Sonne, Isabelle Khurshudyan, Serhiy Morgunov, and Kostiantyn Khudov, "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital," *Washington Post*, August 24, 2022, https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/. "Cyber" is mentioned in passing in Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf; and Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V. Danylyuk, and Nick Reynolds, "Preliminary Lessons in Conventional Warfighting From Russia's Invasion of Ukraine: February–July 2022," Royal United Services Institute, November 20, 2022, https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

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

4 Nadiya Kostyuk and Aaron Brantly, "War in the Borderland Through Cyberspace: Limits of Defending Ukraine Through Interstate Cooperation," *Contemporary Security Policy* 43, no. 2 (2022): 498–515, https://www.tandfonline.com/doi/pdf/10.1080/13523260.2022.2093587.

5 "Ukraine Conflict: Cyberattacks, Frequently Asked Questions," CyberPeace Institute, June 16, 2022, https://cyberpeaceinstitute.org/news/ukraine-conflict-cyberattacks-frequently-asked-questions/.

6 Dustin Volz and Robert McMillan, "In Ukraine, a 'Full-Scale Cyberwar' Emerges," *Wall Street Journal*, April 12, 2022, https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203; and "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

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

8 Jeremy Fleming, "The Head of GCHQ Says Vladimir Putin Is Losing the Information War in Ukraine," *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.

9 Nahal Toosi, Alexander Ward, and Maggie Miller, "Fear and Loathing in Aspen," *Politico*, July 23, 2022, https://www.politico.com/news/2022/07/23/iran-russia-ukraine-defense-aspen-00047550.

10 Raphael Satter, "Satellite Outage Caused 'Huge Loss in Communications' at War's Outset —Ukrainian Official," Reuters, March 15, 2022, https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/; and Dustin Volz and Robert McMillan, "In Ukraine, a 'Full-Scale Cyberwar' Emerges," *Wall Street Journal*, April 12, 2022, https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203.

11 Kim Zetter, "Viasat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Official Says," Zero Day, September 26, 2022, https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact; and Dustin Volz and Robert McMillan, "In Ukraine, a 'Full-Scale Cyberwar' Emerges," *Wall Street Journal*, April 12, 2022, https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203.

12 Dmitri Alperovitch, Twitter post, August 24, 2022, 6:02 p.m., https://twitter.com/DAlperovitch/status/1562560980105584640; and James A. Lewis, "Cyber War and Ukraine," Center for Strategic and International Studies, June 16, 2022, https://www.csis.org/analysis/cyber-war-and-ukraine.

13 Ciaran Martin, "Cyber Realism in a Time of War," Lawfare, March 2, 2022, https://www.lawfareblog.com/cyber-realism-time-war. Updating his assessment in November, Martin said that cyber operations during the Russia-Ukraine war have been "intense and important" while nevertheless showing "severe limitations . . . as a wartime capability." "Lessons From Russia's Cyber-war in Ukraine," *Economist*, November 30, 2022, https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine.

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

15 Joint Chiefs of Staff, "Joint Publication 3-0: Joint Operations," October 22, 2018, https://irp.fas.org/doddir/dod/jp3_0.pdf. The "fires" construct may or may not be how Russia conceptualizes its own military cyber effects operations in Ukraine. This paper's use of the term therefore presents some risk of mirror-imaging—that is, seeing Russia through a U.S. or Western lens, rather than as Russia sees itself. However, the paper's primary aim is to inform Western policymaking; mapping the Russia-Ukraine war onto Western frameworks can help to generate insights and recommendations directly relevant to Western militaries. Additionally, Gavin Wilde has argued that Russia's own holistic doctrine of "information warfare" is "overinflated" and premised on a "conspiratorial mindset" that "superimpos[es] a linear logic to conflict and attribute[s] far more control and intentionality . . . than was ever truly warranted." Wilde warns Western analysts "not to conflate the self-reinforcing logic of that concept with operational coherence, much less strategic impact." To be sure, Westerners must look to Russian concepts when interpreting and predicting Russian decisions. But these concepts aren't the only, or necessarily the best, tools for assessing the impact of Russian actions. See Gavin Wilde, "Assess Russia's Cyber Performance Without Repeating Its Past Mistakes," War on the Rocks, July 21, 2022, https://warontherocks.com/2022/07/assess-russias-cyber-performance-without-repeating-its-past-mistakes/.

16 Technically, the preferred term in U.S. doctrine is "cyberspace attack," considered "a form of fires." Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf. But cyberspace attack is unfortunately similar to the generic term "cyber attack," a notoriously ambiguous phrase that causes frequent miscommunication and lacks clear military connotation. This paper therefore refers to cyber fires.

17 Joshua Rovner, "Cyber War as an Intelligence Contest," War on the Rocks, September 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

18 Julian E. Barnes, "U.S. Lacks a Clear Picture of Ukraine's War Strategy, Officials Say," *New York Times*, June 8, 2022, https://www.nytimes.com/2022/06/08/us/politics/ukraine-war-us-intelligence.html; and Sean Lyngaas, "Russian Missile Strikes Overshadow Cyberattacks as Ukraine Reels From Blackouts, CNN, November 5, 2022, https://www.cnn.com/2022/11/05/politics/russia-cyber-attacks-missiles-ukraine-blackouts/index.html.

19 Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.

20 Suzanne Smalley, "Cybersecurity Experts Question Microsoft's Ukraine Report," CyberScoop, July 1, 2022, https://www.cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/.

21 Ryan Brobst, John Hardie, and Bradley Bowman, "Non-NATO Sources of Soviet and Russian Arms for Ukraine," Foundation for Defense of Democracies, July 6, 2022, https://www.fdd.org/analysis/2022/07/06/non-nato-sources-of-soviet-and-russian-arms-for-ukraine/; 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 (Summer 2022): 113–126, http://dx.doi.org/10.26153/tsw/42073.

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

23 Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf.

24 "KA-SAT Network Cyber Attack Overview," Viasat, March 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

25 "KA-SAT Network Cyber Attack Overview," Viasat, March 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

26 James Pearson, Raphael Satter, Christopher Bing, and Joel Schectman, "Exclusive: U.S. Spy Agency Probes Sabotage of Satellite Internet During Russian Invasion, Sources Say," Reuters, March 11, 2022, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/.

27 Christopher Miller, Mark Scott, and Bryan Bender, "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground," *Politico*, June 9, 2022, https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039.

28 James Pearson, Raphael Satter, Christopher Bing, and Joel Schectman, "Exclusive: U.S. Spy Agency Probes Sabotage of Satellite Internet During Russian Invasion, Sources Say," Reuters, March 11, 2022, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/; "Surfbeam2 Blackout, What Happened With KA-SAT?," SEKOIA.IO, March 7, 2022, https://f.hubspotusercontent10.net/hubfs/7095517/%5BMarketing%5D%20-%20Ebook-analyse/TLP_WHITE_FLINT%202022-015%20-%20Surfbeam2%20black-out%2C%20what%20happened%20with%20KA-SAT.pdf; and Ellen Nakashima, "Russian Military Behind Hack of Satellite Communication Devices in Ukraine at War's Outset, U.S. Officials Say," *Washington Post*, March 24, 2022, https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/.

29 Raphael Satter, "Satellite Outage Caused 'Huge Loss in Communications' at War's Outset —Ukrainian Official," Reuters, March 15, 2022, https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/; and Dustin Volz and Robert McMillan, "In Ukraine, a 'Full-Scale Cyberwar' Emerges," *Wall Street Journal*, April 12, 2022, https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203.

30 Kim Zetter, "Viasat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Official Says," Zero Day, September 26, 2022, https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact.

31 Paul Sonne, Isabelle Khurshudyan, Serhiy Morgunov, and Kostiantyn Khudov, "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital," *Washington Post*, August 24, 2022, https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/.

32 Dan Rice, "The Untold Story of the Battle for Kyiv," Small Wars Journal, May 31, 2022, https://smallwarsjournal.com/jrnl/art/untold-story-battle-kyiv; and Jack Watling and Nick Reynolds, "Operation Z: The Death Throes of an Imperial Delusion," Royal United Services Institute, April 22, 2022, https://static.rusi.org/special-report-202204-operation-z-web.pdf.

33 Thomas Brewster, "As Russia Invaded, Hackers Broke Into a Ukrainian Internet Provider. Then Did It Again as Bombs Rained Down," *Forbes*, March 10, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/; and NetBlocks, Twitter post, February 23, 2022, 11:47 p.m., https://twitter.com/netblocks/status/1496708402755559424.

34 Melanie Mingas, "Ukrtelecom Restores 85% of Services After 'Powerful Cyberattack,'" Capacity, March 29, 2022, https://www.capacitymedia.com/article/29wch971qqy0z3dyifx8g/ukrtelecom-restores-85-of-services-after-powerful-cyberattack.

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

36 "Internet Disruptions Registered as Russia Moves in on Ukraine," Netblocks, February 24, 2022, https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.

37 Melanie Mingas, "Ukrtelecom Restores 85% of Services After 'Powerful Cyberattack,'" Capacity, March 29, 2022, https://www.capacitymedia.com/article/29wch971qqy0z3dyifx8g/ukrtelecom-restores-85-of-services-after-powerful-cyberattack; Nadiya Kostyuk and Erik Gartzke, "Cyberattacks Have Yet to Play a Significant Role in Russia's Battlefield Operations in Ukraine –Cyberwarfare Experts Explain the Likely Reasons," The Conversation, April 4, 2022, https://theconversation.com/cyberattacks-have-yet-to-play-a-significant-role-in-russias-battlefield-operations-in-ukraine-cyberwarfare-experts-explain-the-likely-reasons-178604; and Drew FitzGerald, "In Ukraine War, Keeping Phones Online Becomes Key Defense," *Wall Street Journal*, March 24, 2022, https://www.wsj.com/articles/in-ukraine-war-keeping-phones-online-becomes-key-defense-11648123200.

38 Thomas Brewster, "Ukraine's Engineers Battle to Keep the Internet Running While Russian Bombs Fall Around Them," *Forbes*, March 22, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/.

39 Peggy Kelly and Bruce Sussman, "Ukraine Cybersecurity Leader Shares Defense Insights From Cyber and Physical Front Lines," BlackBerry Blog, October 27, 2022, https://blogs.blackberry.com/en/2022/10/ukraine-cybersecurity-leader-shares-defense-insights-from-cyber-and-physical-fronts.

40 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

41 "Four Months of War: Cyberattack Statistics" (English version), State Service of Special Communications and Information Protection of Ukraine, June 30, 2022, https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak.

42 Vitor Ventura, "Wiper Malware: Attacking From Inside," Talos, May 8, 2018, https://www.talosintelligence.com/resources/58.

43 This excludes ransomware, which is designed to hold files hostage rather than permanently destroy them.

44 To be sure, some prior attacks (like WannaCry and NotPetya) spread wildly, affecting hundreds or thousands of individual victim organizations in a single incident. See Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

45 Ioan Iacob and Iulian Madalin Ionita, "The Anatomy of Wiper Malware, Part 1: Common Techniques," CrowdStrike, August 12, 2022, https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/.

46 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK; Dan Black, Twitter post, November 10, 2022, 11:22 a.m., https://twitter.com/DanWBlack/status/1590741781771354112; Andy Greenberg, "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless," *Wired*, November 10, 2022, https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/; and Max Smeets, Twitter post, July 20, 2022, 8:11 a.m., https://twitter.com/Maxwsmeets/status/1549728801332019202.

47 Gergely Revay, "An Overview of the Increasing Wiper Malware Threat," Fortinet, April 28, 2022, https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat; and Max Smeets, Twitter post, July 20, 2022, 8:11 a.m., https://twitter.com/Maxwsmeets/status/1549728801332019202.

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

49 "Special Report: Ukraine," Microsoft, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

50 Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.

51 Figure 1 aims to paint a very general picture of rough patterns and orders of magnitude seen in multiple data sources; it should not be understood as quantitatively precise. To enable side-by-side comparisons of disparate data, certain data points have been averaged or occasionally interpolated, as explained below. This results in some loss of fidelity, including a possible smoothing of peaks and valleys.
Microsoft data on the number of organizations attacked were assembled from three different reports. Weeks 1-6 come from "Special Report: Ukraine," Microsoft, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd. This report provided a week-by-week victim tally, with thirty-seven organizations in total, through Week 6. The next tranche of data comes from "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK. This second report provided an updated total of forty-eight victim organizations, without a week-by-week breakdown. Assuming the report was up to date as of its release, these figures imply eleven new victims over eleven weeks, averaged here as one attack each in Weeks 7-17.
The final Microsoft data come from Clint Watts, "Preparing for a Russian Cyber Offensive Against Ukraine This Winter," Microsoft, December 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/. Here, Microsoft gave its latest estimate that "roughly 50 Ukrainian organizations" had been victimized by Russian destructive malware as of mid-October. Since late June total was already forty-eight, the mid-October total of "roughly 50" indicates no more than a few new victims during the intervening months. The report separately described a "spike" of destructive attacks in October "after two months of little to no wiper activity." However, the spike would necessarily be small given the similar June and October totals. Microsoft's latest report did not give a full timeline of destructive attacks since June, but it did specifically mention an October 11 ransomware attack against two Ukrainian organizations, and an October 16 destructive attack "against critical infrastructure along the Dniester and Dnieper rivers." (It also mentioned other times in October when Russia "staged" destructive malware, but Microsoft did not say these incidents culminated in successful attacks.) Figure 1 seeks to give a rough reconciliation of all these data points. It posits that Microsoft identified no victimized organizations between Weeks 18 and 32, two victims in Week 33 (the October 11 attack) and two more in Week 34 (an interpretation of the October 16 attack). This brings the total number of organizations attacked to fifty-two (or "roughly 50").
CyberPeace Institute data come from "Timeline," CyberPeace Institute, accessed November 13, 2022, https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline. This figure includes cyber incidents carried out by all perpetrators.
Mandiant data on the number of attacks and malware variants come from Gabby Roncone's and John Wolfram's presentation at CYBERWARCON on November 10, 2022, as documented in Dan Black, Twitter post, November 10, 2022, 11:22 a.m., https://twitter.com/DanWBlack/status/1590741781771354112; and Andy Greenberg, "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless," *Wired*, November 10, 2022, https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/. Mandiant's original data were broken down by month. To render these comparable to Microsoft and CyberPeace Institute data, Mandiant numbers here have been converted to weekly averages, which were rounded in cases when a month's beginning/end did not land neatly on a week's beginning/end.
Microsoft data on destructive malware families come in part from its April 27 report. The first date of use for each malware family is taken from the same source as well as from Pawel Knapczyk, "Overview of the Cyber Weapons Used in the Ukraine-Russia War," Trustwave, August 18, 2022, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/. Microsoft's June 22 report listed the same eight families as its April 27 report, implying that no new malware families had emerged between Weeks 7 and 17.

52 "Statistics of Cyber Attacks on Ukrainian Critical Information Infrastructure: 15–22 March," State Service of Special Communications and Information Protection of Ukraine, March 25, 2022, https://cip.gov.ua/en/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya. Zhora said that the number of attempted "attacks" was growing, but that "most of them are unsuccessful."

53 Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.

54 Andy Greenberg, "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless," *Wired*, November 10, 2022, https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/.

55 Peggy Kelly and Bruce Sussman, "Ukraine Cybersecurity Leader Shares Defense Insights From Cyber and Physical Front Lines," BlackBerry Blog, October 27, 2022, https://blogs.blackberry.com/en/2022/10/ukraine-cybersecurity-leader-shares-defense-insights-from-cyber-and-physical-fronts.

56 Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf; Phil Stewart, "Exclusive: U.S. Assesses up to 60% Failure Rate for Some Russian Missiles, Officials Say," Reuters, March 25, 2022, https://www.reuters.com/business/aerospace-defense/exclusive-us-assesses-up-60-failure-rate-some-russian-missiles-officials-say-2022-03-24/; and Aila Slisco, "Russia Has Fired 1,300 Missiles in Ukraine This War, More Strikes Expected," *Newsweek*, April 26, 2022, https://www.newsweek.com/russia-has-fired-1300-missiles-ukraine-this-war-more-strikes-expected-1701267.

57 Andy Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *Wired*, April 12, 2022, https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.

58 "Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)" (via Google Translate), Computer Emergency Response Team of Ukraine, April 12, 2022, https://cert.gov.ua/article/39518.

59 "Industroyer2: Industroyer Reloaded," ESET, April 12, 2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

60 Kate Conger, "Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid," *New York Times*, April 12, 2022, https://www.nytimes.com/2022/04/12/us/politics/ukraine-russian-cyberattack.html.

61 "Viktor Zhora," Digital Peace Now, June 22, 2022, https://digitalpeacenow.org/stillvulnerable-viktor-zhora/.

62 "ESET Research Jointly Presents Industroyer2 at Black Hat USA With Ukrainian Government Representative," press release, ESET, August 25, 2022, https://www.eset.com/int/about/newsroom/press-releases/events/eset-research-jointly-presents-industroyer2-at-black-hat-usa-with-ukrainian-government-representativ/.

63 Patrick Howell O'Neill, "Russian Hackers Tried to Bring Down Ukraine's Power Grid to Help the Invasion," *MIT Technology Review*, April 12, 2022, https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/.

64 "Enemy Launches Hacker Attacks on the Power System," press release, DTEK, July 1, 2022, https://dtek.com/en/media-center/news/vslid-za-raketnimi-udarami-po-tes-vorog-zavdae-khakerskikh-udariv-po-energosistemi/.

65 PowerOutage.com, Twitter posts, 2022, https://twitter.com/poweroutage_com; Carly Olson, "Ukraine Says Russia Is Retaliating by Hitting Critical Infrastructure, Causing Blackouts," *New York Times*, September 11, 2022, https://www.nytimes.com/2022/09/12/world/ukraine-power-blackout.html; "Eastern Ukraine Suffers Blackout, Kyiv Blames Russia," Al Jazeera, September 11, 2022, https://www.aljazeera.com/news/2022/9/11/ukraines-east-reports-blackouts-water-cuts-officials; and Sean Lyngaas, "Russian Missile Strikes Overshadow Cyberattacks as Ukraine Reels From Blackouts," CNN, November 5, 2022, https://www.cnn.com/2022/11/05/politics/russia-cyber-attacks-missiles-ukraine-blackouts/index.html.

66 Pjotr Sauer and Andrew Roth, "'It Was Worse Than Hell': Life in Mariupol Under Russian Occupation," *Guardian*, June 16, 2022, https://www.theguardian.com/world/2022/jun/16/ukraine-life-in-mariupol-under-russian-occupation; and Asami Terajima, "Over 100,000 Mariupol Residents Trapped in Dire Conditions Under Russian Occupation," *Kyiv Independent*, August 12, 2022, https://kyivindependent.com/national/over-100-000-mariupol-residents-trapped-in-dire-conditions-under-russian-occupation.

67 Rob Picheta and Tim Lister, "Zelensky Accuses Moscow of Energy 'Terrorism' as Russian Strikes Knock out Power for Millions," CNN, November 4, 2022, https://www.cnn.com/2022/11/04/europe/ukraine-energy-terrorism-zelensky-russia-intl.

68 Dmitri Alperovitch, Twitter post, Aug 24, 2022, 6:02 p.m., https://twitter.com/DAlperovitch/status/1562560980105584640.

69 Dana Priest, "NSA Growth Fueled by Need to Target Terrorists," *Washington Post*, July 21, 2013, https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html; and Jeremy Scahill and Glenn Greenwald, "The NSA's Secret Role in the U.S. Assassination Program," The Intercept, February 10, 2014, https://theintercept.com/2014/02/10/the-nsas-secret-role/.

70 "Operation Orchard/Outside the Box (2007)" in *International Cyber Law: Interactive Toolkit*, ed. Kubo Mačák, Tomáš Minárik, and Taťána Jančárková, September 17, 2021, accessed November 16, 2022, https://cyberlaw.ccdcoe.org/wiki/Operation_Orchard/Outside_the_Box_(2007).

71 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

72 "Enemy Launches Hacker Attacks on the Power System," press release, DTEK, July 1, 2022, https://dtek.com/en/media-center/news/vslid-za-raketnimi-udarami-po-tes-vorog-zavdae-khakerskikh-udariv-po-energosistemi/.

73 Sean Lyngaas, "Russian Hackers Allegedly Target Ukraine's Biggest Private Energy Firm," CNN, July 5, 2022, https://www.cnn.com/2022/07/01/politics/russia-ukraine-dtek-hack/index.html; and "XakNet Interview: Exclusive Interview With Pro-Russian Hackers 'XakNet Team' Specially for Russian OSINT," Treadstone 71, June 26, 2022, https://cybershafarat.com/2022/10/31/xaknet-kremlin-proxy-given-specific-instructions-to-hack-kropyva-ddos-telegram/2/.

74 Victor Zhora, Twitter post, July 1, 2022, 9:13 a.m., https://twitter.com/VZhora/status/1542858906560512000.

75 "To Investors & Partners," DTEK, accessed November 16, 2022, https://energo.dtek.com/en/ir/#key_indicators.

76 "Integrated Report 2020: Financial and Non-Financial Results," DTEK, 2021, https://dtek.com/content/announces/dtek_ar_2020_en_web_plus1_file_download_s1182_t4655_i6801_orig.pdf.

77 "The Russian Occupiers Shelled the Kryvorizka TPP: There Is Considerable Destruction" (via Google Translate), Rivne Media, April 27, 2022, https://rivne.media/news/rosiyski-okupanti-obstrilyali-krivorizku-tes-e-znachni-ruynuvannya.

78 "Thermal Power Plants Shelling May Cause Ecological Catastrophe," Rubryka, July 27, 2022, https://rubryka.com/en/2022/07/27/obstrily-tets-mozhut-pryzvesty-do-ekologichnoyi-katastrofy/.

79 Kateryna Stepanenko, Layne Philipson, Katherine Lawlor, Karolina Hird, and Frederick W. Kagan, "Russian Offensive Campaign Assessment, August 2," Institute for the Study of War, August 2, 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-2.

80 Karolina Hird, Kateryna Stepanenko, Frederick W. Kagan, and Grace Mappes, "Russian Offensive Campaign Assessment, June 30," Institute for the Study of War, June 30, 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-june-30; and Kateryna Stepanenko, Karolina Hird, Frederick W. Kagan, and George Barros, "Russian Offensive Campaign Assessment, July 1," Institute for the Study of War, July 1, 2022, https://understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-1.

81 Ruslan Kermach, "The Ukrainian Electric Power Industry on the Front Line: Challenges and Opportunities Ahead," *New Eastern Europe*, May 3, 2022, https://neweasterneurope.eu/2022/05/03/the-ukrainian-electric-power-industry-on-the-front-line-challenges-and-opportunities-ahead/.

82 "Enemy Launches Hacker Attacks on the Power System," press release, DTEK, July 1, 2022, https://dtek.com/en/media-center/news/vslid-za-raketnimi-udarami-po-tes-vorog-zavdae-khakerskikh-udariv-po-energosistemi/.

83 "Special Report: Ukraine," Microsoft, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

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

85 Clint Watts, "Preparing for a Russian Cyber Offensive Against Ukraine This Winter," Microsoft, December 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

86 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

87 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

88 Tim Lister, Gianluca Mezzofiore, Paul Murphy, Laura Smith-Spark, and Rob Picheta, "Russia Widens Attack on Ukraine's Cities, Striking Western Airfields and Dnipro," CNN, March 11, 2022, https://www.cnn.com/2022/03/11/europe/russia-invasion-ukraine-03-11-intl/index.html.

89 Carole Landry, "More Cities Bombarded," *New York Times*, March 11, 2022, https://www.nytimes.com/2022/03/11/briefing/russia-ukraine-attacked-cities.html; "Scenes From an Invasion: Russia Launches Long-Predicted Attack Against Ukraine," RadioFreeEurope/RadioLiberty, February 24, 2022, https://www.rferl.org/a/ukraine-russia-attack-photographs-invasion/31720168.html; and Christopher Miller, "How Dnipro's Tough-talking Mayor Keeps His City on a War Footing," *Politico*, July 29, 2022, https://www.politico.com/news/2022/07/29/dnipros-mayor-ukraine-00048798.

90 Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 90–113, https://www.jstor.org/stable/26481911.

91 "Ukraine Conflict Update 16," Institute for the Study of War, March 6, 2022, https://www.understandingwar.org/backgrounder/ukraine-conflict-update-16; and Matilda Kuklish and Jake Kwon, "1 Killed in Airstrikes Near Preschool and Apartment Building in Dnipro, Ukrainian Authorities Say," CNN, March 11, 2022, https://www.cnn.com/europe/live-news/ukraine-russia-putin-news-03-11-22/h_052f8275998a1734c2f5638e414b198e.

92 William Ralston, "The Untold Story of a Cyberattack, a Hospital and a Dying Woman," *Wired*, November 11, 2020, https://www.wired.co.uk/article/ransomware-hospital-death-germany; Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116; and Joseph Marks, "The Cybersecurity 202: This Was the Month Cyberattacks Turned Fatal," *Washington Post*, September 23, 2020, https://www.washingtonpost.com/politics/2020/09/23/cybersecurity-202-this-was-month-cyberattacks-turned-fatal/.

93 Mason Clark, George Barros, and Kateryna Stepanenko, "Russian Offensive Campaign Assessment, March 12," Institute for the Study of War, March 12, 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-12; Mason Clark, George Barros, and Kateryna Stepanenko, "Russian Offensive Campaign Assessment, March 13," Institute for the Study of War, March 13, 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-13; and Mason Clark, George Barros, and Kateryna Stepanenko, "Russian Offensive Campaign Assessment, March 14," Institute for the Study of War, March 14, 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-14.

94 Mason Clark, George Barros, and Karolina Hird, "Russian Offensive Campaign Assessment, April 1," Institute for the Study of War, April 1, 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-1.

95 "Ukraine Conflict Updates," Institute for the Study of War, accessed November 15, 2022, https://www.understandingwar.org/backgrounder/ukraine-conflict-updates; and Christopher Miller, "How Dnipro's Tough-talking Mayor Keeps His City on a War Footing," *Politico*, July 29, 2022, https://www.politico.com/news/2022/07/29/dnipros-mayor-ukraine-00048798.

96 Joint Chiefs of Staff, "Methodology for Combat Assessment," March 8, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/cjcsi_3162_02.pdf?ver=2019-03-13-092459-350.

97 Sources can be found in the surrounding text. Additionally, for Ukrainian equipment and personnel losses, see Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf; and Stew Magnuson, "BREAKING: Ukraine to U.S. Defense Industry: We Need Long-range, Precision Weapons," *National Defense*, June 15, 2022, https://www.nationaldefensemagazine.org/articles/2022/6/15/ukraine-to-us-defense-industry-we-need-long-range-precision-weapons.
For the impact of Russian electronic warfare, see Thomas Withington, "Russia's Electronic Warfare Capabilities Have Had Mixed Results Against Ukraine," The Drive, June 16, 2022, https://www.thedrive.com/the-war-zone/this-is-whats-happened-so-far-in-ukraines-electronic-warfare-battle; Jack Watling and Nick Reynolds, "Operation Z: The Death Throes of an Imperial Delusion," April 22, 2022, https://static.rusi.org/special-report-202204-operation-z-web.pdf; and Dan Rice, "The Untold Story of the Battle for Kyiv," Small Wars Journal, May 31, 2022, https://smallwarsjournal.com/jrnl/art/untold-story-battle-kyiv.
For telecoms disruptions and their impact, see "Internet Disruptions Registered as Russia Moves in on Ukraine," Netblocks, February 24, 2022, https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K; and Christopher Miller, Mark Scott, and Bryan Bender, "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground," *Politico*, June 9, 2022, https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039.
For electrical infrastructure damage, see PowerOutage.com, Twitter posts, 2022, https://twitter.com/poweroutage_com; Carly Olson, "Ukraine Says Russia Is Retaliating by Hitting Critical Infrastructure, Causing Blackouts," *New York Times*, September 11, 2022, https://www.nytimes.com/2022/09/12/world/ukraine-power-blackout.html; "Eastern Ukraine Suffers Blackout, Kyiv Blames Russia," Al Jazeera, September 11, 2022, https://www.aljazeera.com/news/2022/9/11/ukraines-east-reports-blackouts-water-cuts-officials; Sean Lyngaas, "Russian Missile Strikes Overshadow Cyberattacks as Ukraine Reels From Blackouts," CNN, November 5, 2022, https://www.cnn.com/2022/11/05/politics/russia-cyber-attacks-missiles-ukraine-blackouts/index.html; Pjotr Sauer and Andrew Roth, "'It Was Worse Than Hell': Life in Mariupol Under Russian Occupation," *Guardian*, June 16, 2022, https://www.theguardian.com/world/2022/jun/16/ukraine-life-in-mariupol-under-russian-occupation; and Asami Terajima, "Over 100,000 Mariupol Residents Trapped in Dire Conditions Under Russian Occupation," *Kyiv Independent*, August 12, 2022, https://kyivindependent.com/national/over-100-000-mariupol-residents-trapped-in-dire-conditions-under-russian-occupation.
For artillery impacts, see Andrew S. Bowen, "Russia's War in Ukraine: Military and Intelligence Aspects," Congressional Research Service, September 14, 2022, https://crsreports.congress.gov/product/pdf/R/R47068.

98 David Gauthier-Villars, Steve Stecklow, Maurice Tamman, Stephen Grey, and Andrew Macaskill, "As Russian Missiles Struck Ukraine, Western Tech Still Flowed," Reuters, August 8, 2022, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-missiles-chips/; and "Four Months of War: Cyberattack Statistics" (English version), State Service of Special Communications and Information Protection of Ukraine, June 30, 2022, https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak.

99 Russia had previously disrupted logistics with its 2017 NotPetya cyber attack, which affected the global shipping giant Maersk. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

100 Sources can be found in the surrounding text. Additionally, for information on Russian munitions stockpiles, see Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf.
For a discussion of systemic cyber risk, see David Forscey, Jon Bateman, Nick Beecroft, and Beau Woods, "Systemic Cyber Risk: A Primer," Carnegie Endowment for International Peace, March 7, 2022, https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531. For the lack of "wormable" malware, see "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

101 Lennart Maschmeyer and Myriam Dunn Cavelty, "Goodbye Cyberwar: Ukraine as Reality Check," *Policy Perspectives* 10, no. 3 (May 2022): https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf.

102 Chris Krebs, "The Cyber Warfare Predicted in Ukraine May Be Yet to Come," *Financial Times*, March 20, 2022, https://www.ft.com/content/2938a3cd-1825-4013-8219-4ee6342e20ca.

103 Erica D. Lonergan, Shawn W. Lonergan, Brandon Valeriano, and Benjamin Jensen, "Putin's Invasion of Ukraine Didn't Rely on Cyberwarfare. Here's Why," *Washington Post*, March 7, 2022, https://www.washingtonpost.com/politics/2022/03/07/putins-invasion-ukraine-didnt-rely-cyber-warfare-heres-why/.

104 "Four Months of War: Cyberattack Statistics" (English version), State Service of Special Communications and Information Protection of Ukraine, June 30, 2022, https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak.

105 "Timeline," CyberPeace Institute, accessed November 13, 2022, https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline. This figure includes cyber incidents carried out by all perpetrators. If only those incidents attributed to state actors are considered, the CyberPeace Institute documented nineteen data thefts and eleven destructive cyber attacks.

106 Greg Miller and Catherine Belton, "Russia's Spies Misread Ukraine and Misled Kremlin as War Loomed," *Washington Post*, August 19, 2022, https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/.

107 Sam Sabin and Laurens Cerulus, "Why Ukraine's Phones and Internet Still Work, *Politico*, March 7, 2022, https://www.politico.eu/article/why-ukraines-phones-and-internet-still-work/; 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): 113–126, http://dx.doi.org/10.26153/tsw/42073; and Suzanne Smalley, "Mixed Results for Russia's Aggressive Ukraine Information War, Experts Say," CyberScoop, June 16, 2022, https://www.cyberscoop.com/russia-information-war-ukraine-cyber-command-sorm/.

108 "Special Report: Ukraine," Microsoft, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

109 Elena Grossfeld, "What Does the War in Ukraine Tell Us About Russian Intelligence?," King's College London, March 22, 2022, https://www.kcl.ac.uk/what-does-the-war-in-ukraine-tell-us-about-russian-intelligence.

110 Russia is hardly the first country to misread the political and military situation of a wartime foe. And Western governments also mistakenly expected Russian forces to be able to rout the Ukrainian military. Nevertheless, Moscow's misperceptions and its resulting strategic blunders have been remarkably severe and wide-ranging—among the worst in modern times.

111 Phil Stewart, "Exclusive: U.S. Assesses up to 60% Failure Rate for Some Russian Missiles, Officials Say," *Reuters*, March 25, 2022, https://www.reuters.com/business/aerospace-defense/exclusive-us-assesses-up-60-failure-rate-some-russian-missiles-officials-say-2022-03-24/; and Aila Slisco, "Russia Has Fired 1,300 Missiles in Ukraine This War, More Strikes Expected," *Newsweek*, April 26, 2022, https://www.newsweek.com/russia-has-fired-1300-missiles-ukraine-this-war-more-strikes-expected-1701267.

112 "Russian Strike on the Kyiv TV Tower," Forensic Architecture and the Center for Spatial Technologies, June 10, 2022, https://forensic-architecture.org/investigation/russian-strike-on-kyiv-tv-tower; and Jack Detsch and Robbie Gramer, "Russian Troops Are Taking Putin's Orders to Demilitarize Ukraine Literally," *Foreign Policy*, May 4, 2022, https://foreignpolicy.com/2022/05/04/russia-demilitarize-ukraine-arms-facilities/.

113 Valerie Hopkins, "Missile Strike in Kyiv Rattles Residents After Weeks of Quiet," *New York Times*, June 26, 2022, https://www.nytimes.com/2022/06/26/world/europe/kyiv-missile-strike-ukraine.html.

114 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

115 Christoph Koettl, "Satellite Imagery Provides New Details About an Attack on an Airport in Western Ukraine," *New York Times*, March 8, 2022, https://www.nytimes.com/live/2022/03/08/world/ukraine-russia-war#satellite-imagery-provides-new-details-about-an-attack-on-an-airport-in-western-ukraine; and Christoph Koettl, Brenna Smith, and Drew Jordan, "Videos Capture Russian Cruise Missile Attack on Airport in Western Ukraine," *New York Times*, March 6, 2022, https://www.nytimes.com/live/2022/03/06/world/ukraine-russia#russian-cruise-missile-vinnytsia-airport.

116 Jane Arraf, "Missiles Hit Power Stations in Lviv and Along Crucial Railways in Central and Western Ukraine," *New York Times*, May 3, 2022, https://www.nytimes.com/2022/05/03/world/europe/lviv-ukraine-russia-missiles.html; and "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

117 Paul Sonne, Isabelle Khurshudyan, Serhiy Morgunov, and Kostiantyn Khudov, "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital," *Washington Post*, August 24, 2022, https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/.

118 Clint Watts, "Preparing for a Russian Cyber Offensive Against Ukraine This Winter," Microsoft, December 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

119 "Senior Defense Official Holds a Background Briefing," U.S. Department of Defense, May 4, 2022, https://www.defense.gov/News/Transcripts/Transcript/Article/3020396/senior-defense-official-holds-a-background-briefing/.

120 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

121 Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf.

122 Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf.

123 "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," CrowdStrike, March 23, 2017, https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.

124 Oleksiy Kuzmenko and Pete Cobus, "Cyber Firm Rewrites Part of Disputed Russian Hacking Report," Voice of America, March 24, 2017, https://www.voanews.com/a/cyber-firm-rewrites-part-disputed-russian-hacking-report/3781411.html.

125 Drew Harwell, "Instead of Consumer Software, Ukraine's Tech Workers Build Apps of War," *Washington Post*, March 24, 2022, https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/.

126 Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf.

127 Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf.

128 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): 113–126, http://dx.doi.org/10.26153/tsw/42073.

129 Kyle Mizokami, "Russia Claims It 'Hacked' HIMARS Rocket Launchers. That's Probably a Big, Fat Lie," *Popular Mechanics*, August 24, 2022, https://www.popularmechanics.com/military/weapons/a40958633/russia-claims-it-hacked-himars-rocket-launchers/; and Jack Dutton, "Russian Hackers Target U.S. HIMARS Maker in 'New Type of Attack': Report," *Newsweek*, August 1, 2022, https://www.newsweek.com/russian-hackers-target-us-himars-maker-report-ukraine-russia-1729502.

130 John Hudson, "Ukraine Lures Russian Missiles With Decoys of U.S. Rocket System," *Washington Post*, August 30, 2022, https://www.washingtonpost.com/world/2022/08/30/ukraine-russia-himars-decoy-artillery/.

131 "Read: U.S. Letter to the U.N. Alleging Russia Is Planning Human Rights Abuses in Ukraine," *Washington Post*, February 20, 2022, https://www.washingtonpost.com/context/read-u-s-letter-to-the-u-n-alleging-russia-is-planning-human-rights-abuses-in-ukraine/93a8d6a1-5b44-4ae8-89e5-cd5d328dd150/?itid=lk_inline_manual_4.

132 Greg Miller and Catherine Belton, "Russia's Spies Misread Ukraine and Misled Kremlin as War Loomed," *Washington Post*, August 19, 2022, https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/; and Andrew E. Kramer and Valerie Hopkins, "Zelensky Takes Aim at Hidden Enemy: Ukrainians Aiding Russia," *New York Times*, July 18, 2022, https://www.nytimes.com/2022/07/18/world/europe/zelensky-ukraine-russian-spies.html.

133 Frank Bajak, "A Chilling Russian Cyber Aim in Ukraine: Digital Dossiers," Associated Press, April 28, 2022, https://apnews.com/article/russia-ukraine-technology-business-border-patrols-automobiles-fa3f88e07e51bcaf81bac8a40c4da141.

134 Eric Geller, "Ukraine Prepares to Remove Data From Russia's Reach," *Politico*, February 22, 2022, https://www.politico.com/news/2022/02/22/ukraine-centralized-its-data-after-the-last-russian-invasion-now-it-may-need-to-evacuate-it-00010777.

135 Mansur Mirovalev, "What Is Life Like in Russia-occupied Areas of Ukraine?," Al Jazeera, July 4, 2022, https://www.aljazeera.com/news/2022/7/4/whats-life-like-in-russia-occupied-parts-of-ukraine; Lillian Posner, "A Glimpse at Life Under Russian Occupation," *Foreign Policy*, May 11, 2022, https://foreignpolicy.com/2022/05/11/ukraine-russia-war-occupation-donbas-stanislav-aseyev-prisoner-book-in-isolation/; Nikhil Kumar and Kseniia Lisnycha, "Life Under Russia's Brutal Occupation in Eastern Ukraine: 'You Can Be Shot at Any Moment,'" Grid, June 10, 2022, https://www.grid.news/story/global/2022/06/10/life-under-russias-brutal-occupation-in-eastern-ukraine-you-can-be-shot-at-any-moment/; and Kateryna Semchuk, "Roubles and Repression: How Life in Russian-occupied Kherson is Changing," openDemocracy, April 29, 2022, https://www.opendemocracy.net/en/odr/ukraine-russia-kherson-life-is-changing/.

136 "Ukraine: 'He's Not Coming Back': War Crimes in Northwest Areas of Kyiv Oblast," Amnesty International, May 6, 2022, https://www.amnesty.org/en/documents/eur50/5561/2022/en/.

137 Mansur Mirovalev, "What Is Life Like in Russia-occupied Areas of Ukraine?," Al Jazeera, July 4, 2022, https://www.aljazeera.com/news/2022/7/4/whats-life-like-in-russia-occupied-parts-of-ukraine.

138 Pjotr Sauer and Andrew Roth, "'It Was Worse Than Hell': Life in Mariupol Under Russian Occupation," *Guardian*, June 16, 2022, https://www.theguardian.com/world/2022/jun/16/ukraine-life-in-mariupol-under-russian-occupation.

139 Asami Terajima, "Over 100,000 Mariupol Residents Trapped in Dire Conditions Under Russian Occupation," *Kyiv Independent*, August 12, 2022, https://kyivindependent.com/national/over-100-000-mariupol-residents-trapped-in-dire-conditions-under-russian-occupation.

140 Mansur Mirovalev, "What Is Life Like in Russia-occupied Areas of Ukraine?," Al Jazeera, July 4, 2022, https://www.aljazeera.com/news/2022/7/4/whats-life-like-in-russia-occupied-parts-of-ukraine.

141 Lillian Posner, "A Glimpse at Life Under Russian Occupation," *Foreign Policy*, May 11, 2022, https://foreignpolicy.com/2022/05/11/ukraine-russia-war-occupation-donbas-stanislav-aseyev-prisoner-book-in-isolation/.

142 Adam Satariano and Scott Reinhard, "How Russia Took Over Ukraine's Internet in Occupied Territories," *New York Times*, August 9, 2022, https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html; and "Russia Reroutes Internet Traffic in Occupied Ukraine to Its Infrastructure," Reuters, May 2, 2022, https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/.

143 John Paul Rathbone and Veronika Samborska, "Kherson Counter-offensive Cheered by Ukrainians Enduring Russian Rule, *Financial Times*, September 2, 2022, https://www.ft.com/content/38415880-239c-415e-bd24-63706307204e.

144 "Special Report: Ukraine," Microsoft, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

145 "Timeline," CyberPeace Institute, accessed November 13, 2022, https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

146 Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," *Wired*, March 17, 2022, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.

147 "SSU Exposes Another Bot Farm in Kharkiv (Video)," Security Service of Ukraine, March 31, 2022, https://ssu.gov.ua/en/novyny/sbu-vykryla-novu-vorozhu-botofermu-u-kharkovi-video.

148 Raphael Satter and Dmytro Vlasov, "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts," Associated Press, May 11, 2017, https://apnews.com/article/technology-europe-ukraine-only-on-ap-9a564a5f64e847d1a50938035ea64b8f; and Kenneth R. Rosen, "'Kill Your Commanding Officer': On the Front Lines of Putin's Digital War With Ukraine," *Politico*, February 15, 2022, https://www.politico.com/news/magazine/2022/02/15/10-days-inside-putins-invisible-war-with-ukraine-00008529.

149 John Leicester and David Keyton, "Low Morale Takes Hold of Ukrainian, Russian Troops," NPR, June 19, 2022, https://www.pbs.org/newshour/world/low-morale-takes-hold-of-ukrainian-russian-troops.

150 John Paul Rathbone, Ben Hall, Roman Olearchyk, and Max Seddon, "Military Briefing: Russia's Barrage Hits Ukrainian Morale in the Donbas," *Financial Times*, June 10, 2022, https://www.ft.com/content/506dad4d-6f8e-4952-aa11-32b139d326be.

151 Kareem Fahim, "Russia and Ukraine Agree to Release Blockaded Grain Exports," *Washington Post*, July 22, 2022, https://www.washingtonpost.com/world/2022/07/22/ukraine-grain-deal-turkey-russia/.

152 It is also possible that Moscow and Kyiv never come to any formal agreement. In that case, the hot war would eventually cool into "frozen conflict" of some kind.

153 Raphael Satter, "Ukrainian Officials' Phones Targeted by Hackers —Cyber Watchdog," *Reuters*, June 6, 2022, https://www.reuters.com/world/europe/ukrainian-officials-phones-targeted-by-hackers-cyber-watchdog-2022-06-06/.

154 Kylie Atwood and Zachary Cohen, "US in Contact With Zelensky Through Secure Satellite Phone," CNN, March 1, 2022, https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-02-22/h_6b5c8062541ddb6c36dd43ca70391608; and "The Phones of Ukrainian President Zelensky," Electrospaces, March 28, 2022, https://www.electrospaces.net/2022/03/the-phones-of-ukrainian-president.html.

155 Timothy Bella, "Assassination Plot Against Zelensky Foiled and Unit Sent to Kill Him 'Destroyed,' Ukraine Says," *Washington Post*, March 2, 2022, https://www.washingtonpost.com/world/2022/03/02/zelensky-russia-ukraine-assassination-attempt-foiled/.

156 Paul Sonne, Isabelle Khurshudyan, Serhiy Morgunov, and Kostiantyn Khudov, "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital," *Washington Post*, August 24, 2022, https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/.

157 Sources can be found in the surrounding text.

158 "Fireside Chat on Cyber, Crypto, and Quantum With Anne Neuberger," Aspen Institute, July 20, 2022, https://www.youtube.com/watch?v=wVtoQ2M8KRw.

159 Catherine Stupp, "Russian Cyber Capabilities Have 'Reached Their Full Potential,' Ukrainian Official Says," *Wall Street Journal*, April 27, 2022, https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-04-27/card/russian-cyber-capabilities-have-reached-their-full-potential-ukrainian-official-says-QyH0VEv08BLEI9iPmdlM.

160 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK; and "Microsoft Digital Defense Report 2022," Microsoft, November 4, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv.

161 Clint Watts, "Preparing for a Russian Cyber Offensive Against Ukraine This Winter," Microsoft, December 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

162 "Timeline," CyberPeace Institute, accessed November 13, 2022, https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

163 Valentin Weber, "Financial Incentives May Explain the Perceived Lack of Ransomware in Russia's Latest Assault on Ukraine," Council on Foreign Relations, July 26, 2022, https://www.cfr.org/blog/financial-incentives-may-explain-perceived-lack-ransomware-russias-latest-assault-ukraine; and James Pearson and Raphael Satter, "Analysis: Russian Ransomware Attacks on Ukraine Muted by Leaks, Insurance Woes," Reuters, March 1, 2022, https://www.reuters.com/technology/russian-ransomware-attacks-ukraine-muted-by-leaks-insurance-woes-2022-03-01/.

164 Clint Watts, "Preparing for a Russian Cyber Offensive Against Ukraine This Winter," Microsoft, December 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

165 Sean Lyngaas, "Russian Hackers Behind SolarWinds Breach Continue to Scour US and European Organizations for Intel, Researchers Say," CNN, July 19, 2022, https://www.cnn.com/2022/07/19/politics/russia-solarwinds-hackers.

166 "Microsoft Digital Defense Report 2022," Microsoft, November 4, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv.

167 "Viktor Zhora," Digital Peace Now, June 22, 2022, https://digitalpeacenow.org/stillvulnerable-viktor-zhora/; and Brandon Vigliarolo, "Ukraine's Cyber Chief Comes to Black Hat in Surprise Visit," The Register, August 13, 2022, https://www.theregister.com/2022/08/13/in_brief_security_black_hat/.

168 "Number of Office 365 Company Users Worldwide as of June 2022, by Leading Country," Statista, 2022, https://www.statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country/.

169 Alexander Martin, "Fears Grow of Russian Spies Turning to Industrial Espionage," The Record, September 14, 2022, https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage/.

170 Sean Lyngaas, "Russian Hackers Behind SolarWinds Breach Continue to Scour US and European Organizations for Intel, Researchers Say," CNN, July 19, 2022, https://www.cnn.com/2022/07/19/politics/russia-solarwinds-hackers.

171 Thomas Brewster, "Ukraine's Engineers Battle to Keep the Internet Running While Russian Bombs Fall Around Them," *Forbes*, March 22, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/.

172 Catherine Stupp, "Ukraine Has Begun Moving Sensitive Data Outside Its Borders," *Wall Street Journal*, June 14, 2022, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002; and "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

173 Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf.

174 "Russian Strike on the Kyiv TV Tower," Forensic Architecture and the Center for Spatial Technologies, June 10, 2022, https://forensic-architecture.org/investigation/russian-strike-on-kyiv-tv-tower; and Valerie Hopkins, "Missile Strike in Kyiv Rattles Residents After Weeks of Quiet," *New York Times*, June 26, 2022, https://www.nytimes.com/2022/06/26/world/europe/kyiv-missile-strike-ukraine.html.

175 Mansur Mirovalev, "What Is Life Like in Russia-occupied Areas of Ukraine?," Al Jazeera, July 4, 2022, https://www.aljazeera.com/news/2022/7/4/whats-life-like-in-russia-occupied-parts-of-ukraine; Pjotr Sauer and Andrew Roth, "'It Was Worse Than Hell': Life in Mariupol Under Russian Occupation," *Guardian*, June 16, 2022, https://www.theguardian.com/world/2022/jun/16/ukraine-life-in-mariupol-under-russian-occupation; Lillian Posner, "A Glimpse at Life Under Russian Occupation," *Foreign Policy*, May 11, 2022, https://foreignpolicy.com/2022/05/11/ukraine-russia-war-occupation-donbas-stanislav-aseyev-prisoner-book-in-isolation/; Nikhil Kumar and Kseniia Lisnycha, "Life Under Russia's Brutal Occupation in Eastern Ukraine: 'You Can Be Shot at Any Moment,'" Grid, June 10, 2022, https://www.grid.news/story/global/2022/06/10/life-under-russias-brutal-occupation-in-eastern-ukraine-you-can-be-shot-at-any-moment/; and Kateryna Semchuk, "Roubles and Repression: How Life in Russian-occupied Kherson is Changing," openDemocracy, April 29, 2022, https://www.opendemocracy.net/en/odr/ukraine-russia-kherson-life-is-changing/.

176 "Russia Reroutes Internet Traffic in Occupied Ukraine to Its Infrastructure," Reuters, May 2, 2022, https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/.

177 Emile Aben, "The Resilience of the Internet in Ukraine," RIPE Labs, March 10, 2022, https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine/; and Julian Herbert, "Ukraine IT Sector: Resilient, Agile, and Hopefully Here to Stay," Everest Group, April 14, 2022, https://www.everestgrp.com/blog/ukraine-it-sector-resilient-agile-and-hopefully-here-to-stay-blog.html.

178 Thomas Brewster, "Ukraine's Engineers Battle to Keep the Internet Running While Russian Bombs Fall Around Them," *Forbes*, March 22, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/.

179 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): 113–126, http://dx.doi.org/10.26153/tsw/42073.

180 Jack Watling and Nick Reynolds, "Ukraine at War: Paving the Road From Survival to Victory," Royal United Services Institute, July 4, 2022, https://static.rusi.org/special-report-202207-ukraine-final-web.pdf.

181 "U.S. Support for Connectivity and Cybersecurity in Ukraine," fact sheet, U.S. State Department, May 10, 2022, https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/.

182 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.

183 Eric Geller, "Ukraine Prepares to Remove Data From Russia's Reach," *Politico*, February 22, 2022, https://www.politico.com/news/2022/02/22/ukraine-centralized-its-data-after-the-last-russian-invasion-now-it-may-need-to-evacuate-it-00010777.

184 Author's conversation with the company's CEO, 2022.

185 Joel Schectman and Christopher Bing, "EXCLUSIVE Ukraine Calls on Hacker Underground to Defend Against Russia," Reuters, February 24, 2022, https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/; Stefan Soesanto, "The IT Army of Ukraine: Structure, Tasking, and Ecosystem," ETH Zürich Center for Security Studies, June, 2022, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf; and Lorenzo Franceschi-Bicchierai, "Inside Ukraine's Decentralized Cyber Army," Motherboard, June 19, 2022, https://www.vice.com/en/article/y3pvmm/inside-ukraines-decentralized-cyber-army.

186 Sean Lyngaas, "Russian Hackers Behind SolarWinds Breach Continue to Scour US and European Organizations for Intel, Researchers Say," CNN, July 19, 2022, https://www.cnn.com/2022/07/19/politics/russia-solarwinds-hackers.

187 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK; "Microsoft Digital Defense Report 2022," Microsoft, November 4, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv; "Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future," Amazon, June 9, 2022, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future; Frank Konkel, "Ukraine Tech Chief: Cloud Migration 'Saved Ukrainian Government and Economy,'" Nextgov, December 1, 2022, https://www.nextgov.com/cxo-briefing/2022/12/ukraine-tech-chief-cloud-migration-saved-ukrainian-government-and-economy/380328/; Catherine Stupp, "Ukraine Has Begun Moving Sensitive Data Outside Its Borders," *Wall Street Journal*, June 14, 2022, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002; and Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.

188 Mykhailo Fedorov, Twitter post, July 6, 2022, 3:44 a.m., https://twitter.com/FedorovMykhailo/status/1544588065624178688.

189 Catherine Stupp, "Ukraine Has Begun Moving Sensitive Data Outside Its Borders," *Wall Street Journal*, June 14, 2022, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002; and "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

190 "Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future," Amazon, June 9, 2022, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future; and Catherine Stupp, "Ukraine Has Begun Moving Sensitive Data Outside Its Borders," *Wall Street Journal*, June 14, 2022, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002.

191 "Defending Ukraine: Early Lessons From the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK; and "Microsoft Digital Defense Report 2022," Microsoft, November 4, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv.

192 "Microsoft Digital Defense Report 2022," Microsoft, November 4, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv.

193 For an overview, see 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.

194 Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.

195 Christopher Miller, Mark Scott, and Bryan Bender, "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground," *Politico*, June 9, 2022, https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039.

196 Elizabeth Howell, "Elon Musk Says Russia Is Ramping up Cyberattacks on SpaceX's Starlink Systems in Ukraine," Space.com, October 14, 2022, https://www.space.com/starlink-russian-cyberattacks-ramp-up-efforts-elon-musk.

197 Thomas Brewster, "Ukraine's Engineers Battle to Keep the Internet Running While Russian Bombs Fall Around Them," *Forbes*, March 22, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/; Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486; and Jackie Wattles, "SpaceX Sent Starlink Internet Terminals to Ukraine. They Could Paint a 'Giant Target' on Users' Backs, Experts Say," CNN, March 4, 2022, https://edition.cnn.com/2022/03/03/tech/spacex-starlink-ukraine-internet-security-risks-scn/index.html.

198 Suzanne Smalley, "Mixed Results for Russia's Aggressive Ukraine Information War, Experts Say," CyberScoop, June 16, 2022, https://www.cyberscoop.com/russia-information-war-ukraine-cyber-command-sorm/.

199 Mehul Srivastava, Roman Olearchyk, Felicia Schwartz, and Christopher Miller, "Ukrainian Forces Report Starlink Outages During Push Against Russia," *Financial Times*, October 7, 2022, https://www.ft.com/content/9a7b922b-2435-4ac7-acdb-0ec9a6dc8397.

200 Inga Kristina Trauthig, "Chat and Encrypted Messaging Apps Are the New Battlefields in the Propaganda War," Lawfare, March 27, 2022, https://www.lawfareblog.com/chat-and-encrypted-messaging-apps-are-new-battlefields-propaganda-war.

201 Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.

202 "CYBER101—Cyber Mission Force," press release, U.S. Cyber Command, November 1, 2022, https://www.cybercom.mil/Media/News/Article/3206393/cyber101-cyber-mission-force/; "Quadrennial Defense Review 2014," U.S. Department of Defense, March 2014, https://www.acq.osd.mil/ncbdp/docs/2014_Quadrennial_Defense_Review.pdf; and Martin Matishak and Lara Seligman, "Biden Budget to Seek Boost to the Military's Cyber Force," *Politico*, May 25, 2021, https://www.politico.com/news/2021/05/26/biden-budget-military-cyber-force-490965.

203 "Defense Budget Overview: United States Department of Defense Fiscal Year 2023 Budget Request," U.S. Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, April 2022, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf; and Mark Pomerleau, "Air Force Would Contribute Bulk of New Cyber Mission Force Teams," *Air Force Times*, June 14, 2021, https://www.airforcetimes.com/cyber/2021/06/14/air-force-would-contribute-bulk-of-new-cyber-mission-force-teams/.

204 *United States Special Operations Command and United States Cyber Command: A Hearing Before the Senate Armed Services Committee*, 117th Cong. (2021) (testimony of General Paul M. Nakasone, March 25, 2021), https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-25-21.pdf.

205 *USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings*, U.S. Cyber Command, July 11, 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427; and Sue Gordon and Eric Rosenbach, "America's Cyber-Reckoning: How to Fix a Failing Strategy," *Foreign Affairs*, January/February 2022, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning. For more on cyber force regeneration and the "burning" of cyber tools, see JD Work, "Rapid Capabilities Generation and Prompt Effects in Offensive Cyber Operations," (paper presented at the Annual Conference of the International Studies Association, Las Vegas, April 2021), https://osf.io/preprints/socarxiv/esx6m; and JD Work, "Burned and Blinded: Escalation Risks of Intelligence Loss From Countercyber Operations in Crisis," *International Journal of Intelligence and CounterIntelligence* 35, no. 4 (2022): https://www.tandfonline.com/doi/abs/10.1080/08850607.2022.2081904.

206 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (United Kingdom: Oxford University Press, 2022).

207 "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," U.S. Cyber Command, April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

208 "Weapons Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors," U.S. Government Accountability Office, March 4, 2021, https://www.gao.gov/assets/gao-21-179.pdf; and "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple With Scale of Vulnerabilities," U.S. Government Accountability Office, October 9, 2018, https://www.gao.gov/assets/gao-19-128.pdf.

209 Meredith Roaten, "JUST IN: Mumbai Incident Spotlights China's Cyber Capabilities," *National Defense*, March 3, 2021, https://www.nationaldefensemagazine.org/articles/2021/3/3/mumbai-incident-spotlights-chinas-cyber-capabilities.

210 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.

211 Ash Carter, "A Lasting Defeat: The Campaign to Destroy ISIS," Belfer Center for Science and International Affairs, Harvard Kennedy School, October 2017, https://www.belfercenter.org/publication/lasting-defeat-campaign-destroy-isis.

212 Michael P. Kreuzer, "Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age," The Strategy Bridge, July 8, 2021, https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org