Journal of Strategic Security

Volume 16 | Number 2 Article 7

How Putin's Cyberwar Failed in Ukraine

Austen D. Givens
Utica University, adgivens@utica.edu

Max Gorbachevsky
Utica University, magorbac@utica.edu

Anita C. Biernat
Utica University, acbierna@utica.edu

pp. 96-121

Recommended Citation
Givens, Austen D.; Gorbachevsky, Max; and Biernat, Anita C.. "How Putin's Cyberwar Failed in Ukraine." *Journal of Strategic Security* 16, no. 2 (2023) : 96-121.
DOI: https://doi.org/10.5038/1944-0472.16.2.2099
Available at: https://digitalcommons.usf.edu/jss/vol16/iss2/7

How Putin's Cyberwar Failed in Ukraine

Abstract

As Russian military forces surged across the Ukrainian border in February 2022, cybersecurity analysts shared predictions about the ways in which the Russian government would use cyberattacks to thwart Ukrainian defenses. Some government agencies and private sector organizations forecast that the Russians would launch a blitz of devastating electronic attacks against Ukrainian critical infrastructure targets, such as electrical power plants and air traffic control networks, crippling the country. While Russian cyberattacks have played a role in the conflict, their effects to date have been significantly less than what some analysts anticipated. But why? This article examines how analysts' most extreme predictions about Russia's use of cyberattacks in Ukraine missed the mark, links these findings to the literatures on military and intelligence forecasting, and offers recommendations for additional research.

Acknowledgements

The authors gratefully acknowledge Anthony Spanakos and participants at the Northeastern Political Science Association's 54th annual conference for their comments and suggestions on earlier drafts of this article. We also thank M.B. for editorial assistance and our anonymous reviewers for their helpful feedback.

Introduction

As columns of Russian armored vehicles and soldiers thundered across the Ukrainian border in February 2022, some customers of Viasat, a California-based firm that provides Internet service via satellite, including to customers in Ukraine, experienced a sudden and unexplained signal loss.[1] Special modems that customers use to connect to the Viasat network were remotely wiped and rebooted without warning. These modems were subsequently unable to reconnect to the Viasat network.[2] Among those in Ukraine affected by the attack were the Ukrainian armed forces, which rely in part on Viasat technology for Internet access in remote areas with spotty coverage.[3]

Later independent digital forensic analyses showed that a destructive malicious software application called AcidRain had infected the Viasat customer modems. This software deleted the modems' file systems and triggered a device reboot. That made the modems useless for Viasat customers. Without file systems, modems lack the basic programming to function.[4] Viasat itself offered a slightly different explanation for what took place. The company claimed that an attacker exploited part of its network, then sent legitimate destructive commands that overwrote data on the modems.[5] Both the independent forensic analyses and Viasat's internal investigation, despite their differences, ultimately pointed toward a single coherent narrative: These modems' destruction was not the result of an undetected design flaw or manufacturing defect, but the consequence of intentional action. Someone, somewhere, wanted this to happen.

Three months later, after an exhaustive investigation into the Viasat outage, the European Union, along with the governments of the United Kingdom, United States, Canada, and Australia, all publicly attributed the Viasat outage to an attack by the Russian military intelligence service, known in English as the GRU.[6] This was the first instance of a major, attributed cyberattack against a Ukrainian critical infrastructure target in the 2022 Russian war on Ukraine.

Yet what followed the Viasat outage was even more surprising. To date, there have been no further Russian cyberattacks on Ukraine-connected critical infrastructure that compare to the scope, sophistication, and success of the Viasat incident. The overwhelming majority of damage to

Ukrainian infrastructure has come not through virtual means, but via kinetic weapons—bombs, missiles, and bullets.[7]

It was not supposed to be this way. In the months leading up to the start of the 2022 Russian invasion, western intelligence services, technology firms, and academics warned that Russia could launch potentially crippling cyberattacks on Ukrainian critical infrastructure.[8] In some cases, these forecasts were so dire that citizens of Western nations were themselves warned about the effects of these electronic attacks spilling over to harm individuals and organizations located outside Ukraine, potentially drawing outside states into the conflict as combatants.

To be sure, there has been a continual stream of low-level Russian cyberattacks against Ukrainian military and civilian targets during the conflict, including the use of destructive malware and distributed denial of service (DDoS) attacks. As the authors will show in this article, there is a notable gap between the direst predictions about Russian cyberattacks on Ukraine and that which has transpired on the ground. The impacts of these cyberattacks have been mostly weak. Impressive Ukrainian cyber defense measures have blunted these attacks, contrary to predictions expressed by some Western intelligence services, technology firms, and scholars.

The Russian Ministry of Defense has drastically underperformed expectations in Ukraine, not just in cyber operations, but in other ways, too. It is estimated that over 100,000 Russian soldiers have been killed or injured in Ukraine during the period from February 2022-October 2022.[9] The Ukrainian armed forces say that Russia has lost over 2,500 tanks as of October 2022.[10] Independent media accounts indicate the number of destroyed tanks is at least 1,000.[11] Furthermore, the Russian troops on the ground have not received adequate air support from the Russian Aerospace Forces, which are better known in English as the VKS.[12] Under such conditions, it may seem peculiar to focus narrowly on the shortcomings in Russia's offensive cyber capabilities, since other areas of Russia's armed forces are falling short of expectations, as well.

However, the cyber facets of the Russian invasion merit attention because of the unique attributes of this conflict. The Russian war on Ukraine represents the largest amassing and deployment of troops by one

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

sovereign state, to invade another sovereign state, since World War II.[13] Moreover, the authors believe this is the first multi-domain armed conflict in which the anticipated use of offensive cyber warfare tactics was predicted to be as significant as the use of kinetic weapons.[14] Indeed, cyber operations have evolved from a comparatively small component to an inescapable facet of modern warfare.[15] This evolution means that forecasts about the cyber dimensions of the war were exceptional in a historical sense.

To be sure, there have been excellent scholarly contributions to date in this vein—both about the war in Ukraine, as well as cyber conflict in general. For example, Kostyuk and Gartzke examine Russia's use of offensive cyber operations within the broader spectrum of options available to belligerents in warfare[16]. Martin Libicki of the RAND Corporation has noted that Russia's invasion and occupation of Crimea were notable for the absence of Russian network-centric attacks.[17] Bronk, Collins, and Wallach observe that there were clear differences in Russia's use of cyberattacks in Crimea in 2012, Syria in 2015, and Ukraine in 2022.[18] Other scholars, such as Myriam Dunn Cavelty and Thomas Rid, have written extensively about the evolution of cyber conflict as well as our understanding of what cyber operations may or may not include.[19] While all these works offer useful arguments around the use and efficacy of cyberattacks, the authors' focus in the present article is different. Rather than interrogating the strategic wisdom of cyber operations, assessing their effectiveness in warfare, or coming to grips with how cyber operations influence our understanding of conflict, this article evaluates the role that intelligence analyses played during the 2022 Russian invasion of Ukraine.

This article advances a two-part argument. In so doing, the article contributes to the understanding of intelligence failure, which is a major theme of intelligence studies scholarship, and empirical knowledge about the Russian cyber campaign against Ukraine.[20] The authors will show that the gap between predictions about Russian cyber capabilities and intentions in Ukraine, and what has taken place in Ukraine, represents an intelligence warning failure within the broader taxonomy of intelligence failures advanced by John A. Gentry.[21] As a corollary, this article argues that this intelligence warning failure included a simultaneous overestimation of Russian offensive cyber capabilities and an underestimation of Ukrainian cyber defenses. The article does not address

whether this over-estimation of the Russian cyber threat is desirable, or not, in the formulation of public policy. Empirical evidence from the conflict as well as public statements from United States and Ukrainian government officials support this argument.

The rest of the article proceeds as follows. The first section explores the concept of intelligence failure itself, highlighting scholarly treatments of this subject which focus both on intelligence failures as organizational pathologies and the bureaucratic remedies to reduce them. The second section offers historical evidence of what analysts anticipated could occur in Russia's cyber campaign against Ukraine in 2022. The third section chronicles the observed effects of Russia's actions and explains how these activities were both consistent and inconsistent with analysts' predictions. Next, the article offers five hypotheses, as well as analyses, which help to explain why events in Ukraine have diverged from forecasts about Russia's cyber capabilities. The article concludes with a short list of recommendations for further scholarly research on this subject.

Defining an Intelligence Failure

Analyses of intelligence failure are perhaps the most advanced line of inquiry in the intelligence studies literature. This article defines intelligence as the use of specialized methods and processes for collecting, processing, and analyzing information to determine its significance for U.S. national security interests.[22] As one former Central Intelligence Agency analyst puts it, far from being extraordinary, intelligence failures are normal occurrences, ranging from the trivial to the severe.[23]

Seminal publications on intelligence failure, such as those of Richard Betts, converge on the idea that "failure" is itself misunderstood in some way.[24] A universally accepted definition of intelligence failure does not exist.[25] For this article, following Eiran, intelligence failure is defined as a series of two interrelated events: The presence of a gap between an intelligence service's understanding of reality and actual reality, followed by an event that exposes the gap and harms the national interests of the intelligence service's country.[26]

Intelligence professionals can produce incorrect analyses, whether those analyses are a product of the collection of poor-quality information or

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

inaccurate analyses.[27] In a memorable phrase, Jensen distills this notion as "process versus product."[28] A prominent recent example of this type of failure was the notorious series of analytical breakdowns that led the U.S. Intelligence Community to assert that, in the early 2000s, the government of Iraq was stockpiling weapons of mass destruction (WMDs).[29] Yet such weapons were never located in significant quantities in Iraq following the U.S.-led invasion of Iraq in 2003.[30]

The public understanding of intelligence failures is often a breakdown in the consumption of intelligence. The decision-makers who use intelligence analyses make choices based on those analyses. Those choices can lead to undesirable consequences.[31] Generals commanding an army may choose to shift resources from one location to another, for example, while downplaying the possible risks of this choice—even if the intelligence analyses flag officers consume make those risks abundantly clear. A prime minister may sign a free-trade agreement with a group of nations primarily because it confers certain political advantages, rather than offering significant economic benefits. A regional defense alliance may choose to impose economic sanctions on an adversary nation, rather than engage in armed conflict with that nation because doing so is comparatively inexpensive and demonstrates public resolve—even if the intelligence to which the alliance has access indicates that the odds of the economic sanctions succeeding are low.

A second key theme in the scholarship on intelligence failure is organizational reform.[32] When intelligence failures are significant enough to impose a political cost on elected leaders, those leaders can make efforts to prevent a recurrence of the failures through organizational changes. These modifications are as much political as they are administrative. Organizational changes may help to resolve genuine problems revealed by intelligence failures. These modifications can also be politically useful for elected officials. Changes can demonstrate that elected officials are doing something—anything—to address the source of the failures, manifesting responsiveness to constituent needs and concerns.

Yet organizational reforms after intelligence failures are not inevitable, nor are these reforms always necessary. Well-intended changes can lead to unforeseen consequences that contribute to other intelligence failures in the future.[33] Reforms can include the re-wiring of organizational diagrams,

lateral shifting of personnel, or re-naming of offices and divisions, for example. In more extreme cases, these reforms can spur the creation of all-new organizations, such as the Office of the Director of National Intelligence (ODNI) in 2004, whose establishment was a direct reaction to the 9/11 terrorist attacks.[34]

A third theme of note in research on intelligence failures is the development of taxonomies to define and classify intelligence failures by type. Marrin, for example, analyzes intelligence failures leading to strategic surprise, noting that that term is part of the intelligence lexicon and exists in its own right as part of the security studies literature.[35] Jervis notes that the United States' failure to locate WMD in Iraq during Operation Iraqi Freedom is a case of a disconnect between intelligence estimates and what later was shown to be true.[36]

Some of the more developed scholarship on taxonomies of intelligence failures has been produced by Gentry, who classifies intelligence failures under the following headings: Threat warnings, opportunity warnings (failure to notify decision-makers about a chance to exploit something), threat response (failure to respond to threat warnings), opportunity response (decision-makers fail to exploit opportunities), vulnerability identification (failure to recognize one's own comparative weaknesses in the context of other actors' intentions and capabilities), and vulnerability amelioration (failure to mitigate one's own vulnerabilities).[37]

Gentry's work is useful in the context of the present study, for it helps to clarify the fact that, in the case of Ukraine, the U.S. Intelligence Community's assessment of Russian offensive cyber capabilities is probably best understood as a threat warning, albeit a multi-dimensional one. The scope and severity of the threat described by the U.S. Intelligence Community did not account for the robust cyber protection measures Ukraine established following the Russian invasion of 2014. Thus, the intelligence failure in Ukraine was in equal measure an overestimation of offensive cyber capabilities and an underestimation of cyber defensive capacity.

Moreover, the failure to gauge accurately the strength of Ukraine's cyber defenses and Russia's offensive cyber capabilities raises important questions about underlying organizational pathologies which may have

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

influenced finished intelligence products. There are historic examples of intelligence failures that have led to major organizational reforms, for example.[38] That which transpired in Ukraine does not rise to that level of intelligence failure. Unlike the 9/11 attacks, which directly impacted the United States, the Russian invasion of Ukraine had no such effect on the U.S. homeland. It was, instead, a major Russian offensive against Ukraine, a United States ally.

The failure of cyber intelligence estimates in Ukraine would appear to have more in common with the CIA's inaccurate prediction that the Soviet Union would not attempt to place nuclear weapons in Cuba in September 1962—a failure that would be revealed in dramatic fashion through overflight imagery in October 1962.[39] In revisiting that estimate, Sherman Kent, one of the analysts who authored the original intelligence product indicating that the Soviet Union would not place nuclear weapons in Cuba, wrote: "[L]acking the direct evidence, the authors went to the next best thing, namely, information which might indicate the true course of developments."[40] The underlying processes leading to this finished intelligence product include organizational "tendencies"— fixed ways of being and operating.[41] Analysts also appear to have assumed the worst-case scenario about Ukraine: Namely, that the Russians would cripple Ukraine's fragile, antiquated critical infrastructure through cyberattacks, notwithstanding the comparative strength of Ukrainian cyber defenses.[42]

What Did Analysts Predict in Ukraine?

Documenting what has transpired in Ukraine, and how this has deviated from forecasts about what would occur, is at the heart of this article. This section first explains the methods used to collect data for this analysis, then examines predictions about Russian cyberattacks in Ukraine from government organizations, including intelligence agencies and diplomatic sources. It is important to note that the authors wrote this article using only open-source, unclassified information, it faces certain limitations in its analyses. Government officials publish unclassified intelligence estimates after they remove the most sensitive information within them. This means that the key findings from unclassified intelligence estimates remain consistent with those of classified estimates.[43] Classified intelligence estimates do not, and cannot, fundamentally contradict their unclassified versions. Second, this section explores private sector

predictions about Russian cyberattacks in Ukraine, including information from large technology firms like Microsoft, think tanks, and technology industry publications.

The reports discussed below were located through Internet-based searches for materials published between November 1, 2021, and October 1, 2022, for terms related to forecasts about Russian cyber activities in Ukraine. These included phrases such as "Russian cyberattacks on Ukraine" and "intelligence estimates on Russian cyberattacks in Ukraine," as well as variations of these search terms. The reason that this period was selected is that it was during these months that the possibility of a Russian military invasion of Ukraine became most apparent to Western intelligence agencies, largely due to the rapid build-up of Russian troops and equipment along the Russian-Ukrainian border.[44] It was also chosen because this period includes the first six weeks of the invasion, during which close observations of Russian actions led to refinements in intelligence forecasts about cyber activities. This provides the widest possible analytical window through which to observe and analyze Russian cyber activities. Of particular interest in this search were reports that seemed to go against the general thrust of most articles on this subject—in other words, those articles which downplayed the possible risks posed by Russian cyberattacks, or stressed the comparative strength of Ukraine's cyber defenses vis-à-vis Russian offensive cyber capabilities.

During the period from November 2021 through March 2022, the consensus among Western intelligence agencies—and particularly the Five Eyes group, consisting of the United States, Canada, the United Kingdom, Australia, and New Zealand—was that a wave of crippling Russian cyberattacks against Ukrainian targets was likely.[45] Moreover, these attacks had the potential to affect nations far from the center of the conflict. For example, malware targeted at industrial control systems in power plants has the potential to spill over and affect systems in other industries, such as manufacturing, in unanticipated ways, since manufacturing facilities often use computer systems whose functionality is similar to that of power plants.

In January 2022, the United Kingdom's National Cyber Security Centre (NCSC), a component of the United Kingdom's signals intelligence agency, warned U.K. businesses to harden their network defenses in response to

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

events in Ukraine.[46] The U.S. Cybersecurity and Infrastructure Security Agency (CISA), together with the Federal Bureau of Investigation and National Security Agency , issued a similar cautionary message intended to help U.S. organizations pinpoint specific types of malicious software and tactics, echoing the NCSC's guidance in the United Kingdom.[47] The Australian Cyber Security Centre, Canadian Centre for Cybersecurity, and New Zealand's National Cyber Security Centre issued related advisories for their citizens, too, in February.[48] The common theme to these messages was that while the Five Eyes members were generally unaware of specific threats to their citizens, their prior knowledge of Russian government tactics, techniques, and procedures suggested that citizens within their respective nations should be alert to the possibility of spillover attacks emanating from the Russian-initiated conflict.

The U.S. Cybersecurity and Infrastructure Security Agency, a component of the U.S. Department of Homeland Security, took advantage of the Russian conflict to promote cyber hygiene. Through an initiative called Shields Up, CISA leveraged media attention and concern about Russian cyberattacks to encourage U.S. organizations to improve their cybersecurity posture in a public service announcement-style campaign.[49] Shields Up was clever in its timing and use of contemporary issues to support CISA's mission.

There was also recognition of the degree to which Russian cyberattacks could threaten civilian infrastructure. For example, declassified intelligence shared with the *Washington Post* indicated a hidden Russian presence within Ukrainian computer networks. These penetrations—possibly using sophisticated malicious software designed to obfuscate its presence—would presumably be used to disrupt Ukrainian infrastructure during the Russian-Ukrainian conflict.[50] The Office of the Director of National Intelligence, in its February 2022 Worldwide Threat Assessment—a widely-distributed, unclassified intelligence product—underlined that the U.S. Intelligence Community saw the Russian government as "particularly focused" on its capacity to attack and degrade critical infrastructure targets both in the United States and in allied nations, including Ukraine.[51] Considering this assessment, and combining it with the direct warnings issued by Five Eyes members to their citizens, a few observations are clear. Western intelligence agencies saw Russia's offensive cyber capabilities as sufficiently developed to merit a warning

message to their citizens about potential spillover effects from attacks in Ukraine. In addition, the U.S. Intelligence Community highlighted Russia's determination to target critical infrastructure using cyberattacks.

Private sector warnings about the scope and severity of possible cyberattacks in Ukraine were similarly grim. For example, a team at Johns Hopkins University determined that there was an "extremely high likelihood" of a cyberattack on Ukraine during the conflict.[52] The Johns Hopkins University team defined cyberattack broadly, noting that it can encompass attacks on critical infrastructure or simply exist as a component of broader hybrid warfare.[53] Writing in the *Harvard Business Review* a few weeks after the start of the invasion, Stuart Madnick noted that the cyber conflict between Ukraine and Russia could become so acute as to spill over, potentially drawing in the United States and European Union, for instance, and echoing analyses from western intelligence agencies.[54] At least one industry expert suggested that "The authors could see a coordinated campaign…targeting the Ukrainian government's senior leader communications, military critical infrastructure and communications, and aspects of Ukrainian national critical infrastructure".[55] Like government agencies with a stake in the outcome of the Russian-Ukrainian conflict, private organizations, including technology firms and academic institutions, saw a high risk of Russian cyberattacks in the conflict, the potential for attacks targeting critical infrastructure, and the possibility of the cyber conflict drawing in unwilling third party participants.

What Actually Happened in Ukraine

Although the predictions about possible Russian cyber activities in Ukraine were troubling, it has in fact been kinetic weapons, rather than cyberattacks, that have done the most damage to Ukrainian infrastructure to date.[56] To the extent that cyberattacks have been employed against Ukrainian targets, these attacks have been largely unsophisticated, causing significant inconvenience and alarm, but little in the way of critical disruptions or loss of life. Given the fluid nature of the conflict, however, this could change at any time.

What follows below is an incomplete account of significant cyberattacks and related events that have been recorded in Ukraine since the beginning

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

of the conflict.[57] The authors offer several caveats here to contextualize this information. The purpose of this section is not to catalogue all the cyberattacks that cybersecurity analysts have observed on Ukrainian targets. There is also some unknowable proportion of cyberattacks that have been neither detected by Ukraine's cyber defenses nor recorded and reported on publicly.

While it may be that Russian actions observed to date represent part of a calculated strategy—perhaps a hedging of capabilities for use later—other information belies this possibility. The Russian Ministry of Defense is conscripting civilians to bolster thinning ranks of Russian soldiers on the front lines of the war in Ukraine.[58] This suggests that the Russians did not anticipate correctly the number of troops and quantities of equipment that would be necessary to fight and win in Ukraine. Under such circumstances, the authors doubt that the Russian government would deliberately curtail its cyber capabilities as part of a larger offensive strategy.

It is also important to underline that cybersecurity officials have not verified and attributed to the Russian government all of these attacks using recognized digital forensic investigation tools and methods. There are several good reasons for this. First, investigating the source of the attacks fundamentally draws the same groups of information technology professionals away from the active defense of Ukrainian computer networks and toward post-facto investigation. At the time of the writing, defense, not investigation, is a top priority. A second, bigger reason for the lack of official attribution is that the Ukrainian government likely views it as unnecessary. The organs of Ukraine's defense and security establishment know who is responsible for the cyberattacks. Third, even if the Ukrainians had the time and resources to investigate the sources of these cyberattacks, attack attribution is difficult, even under ideal conditions. Most nation-state actors go out of their way to use third-party proxies, pseudonyms, and technical measures like virtual private networks, to obscure their identities.

Online vandalism and disruption of Ukrainian government websites have been two favored tactics observed since the early stages of the conflict. In January 2022, before the start of the invasion, the websites for the Ministry of Foreign Affairs and Ministry of Energy were knocked offline,

among others.[59] The same month, tech giant Microsoft issued a warning that it had identified destructive malware on "dozens" of computer systems in Ukraine, the purpose of which was to render devices and systems inoperable.[60]

In February 2022, Microsoft again reported that what it suspected were Russian actors had been identified on networks operating critical infrastructure—without specifying the nature of the infrastructure—in Sumy, Ukraine.[61] Later that month, a DDoS attack took down the websites of two Ukrainian banks, temporarily.[62] While DDoS attacks are disruptive and inconvenient, they are not sophisticated. DDoS attacks involve re-directing electronic data requests to a server to overload it and, ultimately, take it offline for a period that can range from a few minutes to a few days.[63] The U.S. government publicly attributed this particular set of attacks to the Russian military intelligence service, the GRU.[64]

In March, Microsoft noted that a Kyiv-based media company was targeted with a form of destructive malware known as DesertBlade.[65] This malicious software is designed first to overwrite, then delete, data on all accessible drives.[66] In this way, if undetected and left to execute without intervention, DesertBlade could theoretically wipe out most files on a government agency, corporate, or university computer network. Also in March, Ukraine's government claimed on Twitter that Russian hackers were executing DDoS attacks "nonstop" against various government sites.[67] Moreover, on March 15th the Secret Service of Ukraine said it arrested an individual who the agency claimed was using Ukrainian telecommunications infrastructure to facilitate phone calls among Russian troops in Ukraine as well as to harass Ukrainian soldiers.[68] This was significant because it suggested that the Russian government was receiving substantial communications assistance from at least one individual located inside Ukraine itself.

April 2022 saw further measures to support the government of Ukraine taken by private actors as well as governments. Meta, the parent company of Facebook, Instagram, and WhatsApp, identified a group called "Ghostwriter" that was using fake online accounts to promote pro-Russian propaganda and distribute disinformation.[69] Ghostwriter's actions could be classified as a form of information warfare in this context, rather than network-centric warfare.[70] Nonetheless, disinformation complements

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

Russian efforts to access and disable Ukrainian electronic systems.[71] In addition, Sandworm, a Russian hacking group, was discovered the same month in the networks of the Ukrainian railway and transportation systems.[72]

Additional incidents filled the spring and summer of 2022, underlining the salience of cyberattacks in the Russia-Ukraine conflict. In May, the U.S. government and its allies publicly linked a February 2022 attack on Viasat, a satellite internet provider, to the GRU. This was one of the few instances during the war in which governments took the time and effort to name the Russian government as the actor behind a specific attack.[73] A June report from Microsoft detailed the firm's analysis of Russian cyber tactics to date in the conflict, noting that Microsoft analysts had seen "multiple waves" of cyberattacks designed to spread destructive malware against nearly 50 different Ukrainian organizations.[74] This suggests that the Russian government was keen to cause widespread disruption across swathes of Ukrainian society, including the business community.

Finally, in midsummer 2022, Ukraine's State Service of Special Communication and Information Protection (SSSCIP), a government agency, released a summary report stating that it recorded a total of 203 cyberattacks during the month of July, with the majority of targeted organizations being government agencies.[75] That same month, CISA and the SSSCIP signed a memorandum of cooperation (MOC) to facilitate intergovernmental collaboration on cybersecurity initiatives.[76] This MOC likely helped to codify existing prior collaboration among the Ukrainian and U.S. governments. It also offered important symbolic support. This can be useful in building inter-organizational partnerships that last.[77] In August, the Security Service of Ukraine announced that it shut down a so-called bot farm. This bot farm used automated account creation and communication tools to disseminate pro-Russian propaganda and disinformation about wartime activities, as well as create false narratives about conflict within the upper echelons of the Ukrainian government.[78]

In sum, between January 2022 and the end of summer 2022, publicly available evidence strongly suggests that the Russian government, or Russian government-affiliated groups, executed a multi-faceted electronic campaign against Ukraine.[79] The goals of this campaign appear to have been to degrade the Ukrainian military's ability to command and control

its responses to the Russian military invasion. Other actions observed included coordinated efforts to spread pro-Russian disinformation and propaganda, limit Ukraine's ability to disseminate information among military units and via traditional media channels, facilitate communication among Russian military units, as well as to harm Ukrainian energy and transportation networks.

How Intelligence Missed the Mark

Russia's actions to date in Ukraine have been broadly consistent with intelligence agencies and private sector actors' early estimates about Russian intentions and interests. This congruence between intelligence predictions and events that unfolded in Ukraine represents an intelligence success. Equally clear is that some of the more extreme predictions about Russian actions have not happened. There have been no spillover conflicts resulting directly from Russia's cyberattacks, for instance. Missiles have done far more damage to Ukrainian infrastructure than any electronic attacks directed from a keyboard.[80]

Governments have begun to acknowledge the shortfalls in Russia's cyber performance, as well as the comparative resilience of Ukraine's cyber defenses. For example, Mieke Eoyang, U.S. Assistant Secretary of Defense for Cyber Policy, has noted that Russia "underperformed expectations" in the cyber domain during the invasion.[81] Sir Jeremy Fleming, head of the U.K.'s Government Communication Headquarters, the U.K.'s signals intelligence agency, wrote that Ukraine's cyber defense had proven stronger than Russia predicted.[82] Victor Zhora, who leads Ukraine's cybersecurity agency, has highlighted the important roles Microsoft and ESET—both technology firms—have played in deploying sensor technology to identify anomalous network activity in Ukraine.[83] These comments all indicate a growing recognition that Russia's cyber activities in Ukraine have not manifested themselves in quite the ways that were anticipated before the invasion.

Beyond these assessments, it is important to note that Ukraine's home-grown cyber defense capabilities are formidable. The Ukrainian Ministry of Science and Education participates in the European Education Initiatives Project, for example, a public-private sector partnership aimed at ensuring domestic IT education meets global standards and best

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

practices.[84] Some Ukrainian tech firms with a physical presence outside Ukrainian borders have remotely assisted Ukrainian cyber defenders located inside Ukraine.[85] Numerous Western governments have delivered direct and indirect assistance to cybersecurity officials inside Ukraine.[86]

With the foregoing analysis in mind, the authors offer five hypotheses that help begin to explain why the worst expectations about Russian cyber activities in Ukraine have not squared fully with reality. While these hypotheses do not have robust explanatory power when considered independently, taken as a whole, offer a first cut at understanding why the more extreme forecasts about Russian cyber actions have not happened.

Hypothesis #1: Western intelligence agencies overestimated Russian cyber capabilities before the invasion

> The strongest evidence for this hypothesis comes from the Five Eyes alliance itself. As noted above, each member state—the United States, Canada, the United Kingdom, Australia, and New Zealand—not only released public warnings about Russian cyber capabilities and intentions in Ukraine. The Five Eyes alliance took the added measure of suggesting to their citizens that Russia's actions could directly impact organizations inside their sovereign borders. Whether these warnings were a product of genuine analysis or a rhetorical tool to induce behavioral change is immaterial. Irrespective of its motivation in this regard, the Five Eyes group saw Russian offensive cyber capabilities as sufficiently threatening to prompt them to alert their citizens about their potential effects. Yet this was, in hindsight, a misjudgment. Thus far Russia's activities in Ukraine have largely been contained to Ukraine. The danger of spillover harm thus far appears to be minimal.
>
> If this hypothesis is correct, then one might characterize over-estimation as a kind of threat warning error. Following Gentry's taxonomy of intelligence failures, what occurred was not a failure to warn generally of Russian cyber capabilities, nor to urge caution about Russian attacks on infrastructure. Instead, western intelligence agencies appear to have perceived a severity of threat level from Russia that, so far, does not square with reality.

Hypothesis #2: Intelligence estimates did not account fully for Ukrainian institutional learning and resilience to defend against cyberattacks

Viewed from the perspective of cyber defense, rather than offense, this hypothesis also seems plausible. Part of forecasting the strength of Russia's offensive cyber warfare capabilities involves reckoning the comparative strength of Ukrainian cyber defenses. While analysts may have put much stock in Russia's abilities, Russia did not account entirely for the measures Ukraine has taken to improve its cyber defenses in recent years. In 2014, Russia used armed forces to annex Crimea, an eastern region of Ukraine. The next year, Russia launched electronic attacks against Ukraine that disrupted electrical power to over 100,000 Ukrainian customers.[87] In the wake of those events, the Ukrainian government, as well as infrastructure owners and operators, took action to improve their cyber defenses. The Five Eyes member governments, as well as prominent technology firms like Microsoft, have provided technical training and assistance to critical infrastructure stakeholders in Ukraine.[88] These activities, combined with the experience of fending off electronic attacks since Russia annexed Crimea in 2014, likely contributed to improved Ukrainian cyber defenses in the present conflict.

Moreover, the Five Eyes governments, technology companies, and the U.S. military have provided tangible aid to support the Ukrainian military's defenses, both directly and indirectly. The United Kingdom publicly attributed the February 2022 attack on Viasat to the Russian government.[89] This sort of attack attribution is only possible following deep digital forensic analyses. The government of the United Kingdom certainly played at least some role in carrying out those forensic analyses, for the task of attributing cyberattacks—particularly when the aggressor actively tries to obfuscate its identity—is notoriously difficult.[90] It is hard to imagine that the United Kingdom would officially declare the attack to be Russian in origin without having conducted its investigation. Microsoft has taken an active role in supporting the Ukrainian government, using networks of globally distributed sensors to identify possible malicious activity on Ukrainian computer networks, then alerting the Ukrainians to the presence of this

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

activity.[91] USCYBERCOM, which is the U.S. Department of Defense's combatant command dedicated to offensive cyber operations, sent personnel to Ukraine last year to educate and train Ukrainian cyber defenders. The deputy head of Ukraine's cyber defense agency publicly credited the assistance of allied governments, including the United States, noting that this aid has helped Ukraine's cyber defenses and improved its resilience during the conflict.[92] All of this institutional learning and growth has made a difference in Ukraine's ability to shield itself from Russian cyberattacks and likely was not weighted as heavily as it should have been in intelligence products before the invasion.

Hypothesis #3: Sensitive to the possibility of a major analytical failure, cybersecurity experts erred on the side of doom

Even if incorrect forecasts about what would happen in Ukraine resulted from basic analytic errors, there remains a fundamental question as to why—rather than how—those analytic errors occurred. It is here that the authors get into speculative territory. It is possible, for example, that the U.S. Intelligence Community's failure to predict the strength of the Taliban seizure of Afghanistan in 2021, which led in part to a calamitous United States exit from that nation, somehow influenced estimates about what Russia could do in Ukraine. Stung by the unanticipated strength of the Taliban's takeover in Afghanistan, and smarting from the political battering they took during the Trump years, leaders within the U.S. Intelligence Community may—even unconsciously—have erred on the side of caution in Ukraine. Although intelligence agencies underestimated the adversary Taliban's strength in Afghanistan, analysts overestimated Russian capabilities against Ukraine. Similarly, analysts underestimated Ukrainian cyber defenses, hedging against their over-estimation of the Afghan government's strength.

This hypothesis is not evidence-based. Since this article is based entirely on open-source, unclassified information, it is impossible to know how, if at all, the intelligence failures in Afghanistan may have influenced analyses of Ukraine. Common sense suggests that U.S. Intelligence Community leaders would have been extra

> sensitive to the possibility of a second major forecasting failure after Afghanistan. It may be that Intelligence Community leaders encouraged analysts—directly or indirectly, consciously, or unconsciously—to ensure that analysts allowed for the worst possible potential outcomes in their intelligence products.

Hypothesis #4: The most skilled Russian IT specialists have been fleeing Russia in droves, leaving less capable professionals behind to conduct cyberattacks against Ukrainian targets

> There is evidence that since the start of the Russian invasion of Ukraine, skilled IT workers have left the country in significant numbers.[93] As of December 2022, one media report indicated that around 100,000 such professionals had emigrated, most of them to countries neighboring Russia.[94] To some degree this out-migration is understandable. During wars, those with the financial means to go abroad to avoid being conscripted often do.[95] Most relevant is that it is plausible that some percentage of those who have fled Russia likely would have been able to contribute to, and carry out, cyberattacks against Ukrainian targets. At least one recent study suggests that those who have left are the most important, capable software developers in Russia, underlining the potential viability of this hypothesis.[96] It is reasonable to assume that those same IT professionals made a conscious decision not to contribute to the war against Ukraine by fleeing Russia. This means that the Russian state has a smaller pool of skilled IT workers from which to draw to engineer and execute cyberattacks against Ukrainian targets.

Hypothesis #5: Western intelligence services' public warnings about Russian plans helped to mitigate the impact of Russian cyberattacks

> It is possible that the extraordinary public airing of intelligence analyses before and during the Russian invasion helped to blunt Russia-sponsored cyberattacks against Ukrainian targets.[97] According to interviews with senior U.S. government officials, the decision to declassify and broadcast publicly intelligence about Russian intentions was designed to pre-empt Russian disinformation about the conflict.[98] This decision likely had secondary effects, as well. For example, Russian war plans may

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

have been disrupted, too, inducing Russia-affiliated groups and individuals to modify their selection of certain electronic targets inside Ukraine. Plotting effective cyberattacks requires advanced reconnaissance. This level of disruption to Russian plans, combined with Ukraine's array of cyber defenses, may have been a critical factor in Russia's underwhelming cyberattacks against Ukrainian targets.

Conclusion

In this article, the authors argued that the gap between the predicted effects of Russian cyberattacks in Ukraine and the true, moderated impacts of those attacks represents an intelligence warning failure. This failure has nuance, however, in that it consists of both an overestimation of Russian cyber capabilities and an underestimation of Ukrainian cyber defenses. These observations contribute to broader theoretical research on intelligence failures, which are an established subject of scholarly interest in intelligence studies. The article's observations also add empirical data about Russian cyberattacks against Ukraine during the 2022 invasion to the body of knowledge, as well.

Further scholarship in this line of inquiry could benefit from additional quantitative data published by the Five Eyes governments, as well as the government of Ukraine, related to the 2022 conflict. A near-full accounting of the cyberattacks launched against Ukraine in 2022 would be impossible to tally since many lower-level attacks likely go unnoticed and unreported. There are also pressing and relevant information security concerns around releasing such data since the conflict itself is ongoing. Even an incomplete, indexed list of attacks, classified by target type, would help expand understanding of Russian target selection. The data may also indicate areas in which Ukrainian cyber defenses are most robust, and where defenses are in most need of further attention.

A second suggestion for future research would be for scholars to investigate Ukrainian cyber defenders' perceptions of their performance, perhaps through semi-structured interviews. Researchers could benefit from surveying Ukrainian cybersecurity officials about how these officials would assess their own performance during the conflict, as well as their thoughts on how effective—or ineffective—the assistance from Western

powers and technology firms has been. While the Russian invasion of Ukraine grinds on, little remains certain. Russian cyberattacks on Ukrainian infrastructure, and robust Ukrainian defenses mounted against them, will continue.

Endnotes

1 Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," *Wired*, March 23, 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/.
2 Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine."
3 Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine."
4 Michael Kan, "Viasat Hack Tied to Data-wiping Malware Designed to Shut Down Modems," *PC Magazine*, March 31, 2022, https://www.pcmag.com/news/viasat-hack-tied-to-data-wiping-malware-designed-to-shut-down-modems.
5 Lee Mathews, "Viasat Reveals How Russian Hackers Knocked Thousands of Ukrainians Offline," *Forbes*, March 31, 2022, https://www.forbes.com/sites/leemathews/2022/03/31/viasat-reveals-how-russian-hackers-knocked-thousands-of-ukrainians-offline/?sh=2f34b42160d6.
6 Council of the European Union, "Russian cyber operations against Ukraine," May 10, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/; William James, "UK Says Russia Was behind February 24 Viasat Cyber Attack," *Reuters,* May 10, 2022, https://www.reuters.com/world/uk/uk-says-russia-was-behind-feb-24-viasat-cyber-attack-2022-05-10/; Global Affairs Canada, "Statement on Russia's Malicious Cyber Activity Affecting Europe and Ukraine," Government of Canada, May 9, 2022, https://www.canada.ca/en/global-affairs/news/2022/05/statement-on-russias-malicious-cyber-activity-affecting-europe-and-ukraine.html; Karen Andrews, "Attribution to Russia for Malicious Cyber Activity against European Networks," Minister for Foreign Affairs (Austria), May 10, 2022, https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-russia-malicious-cyber-activity-against-european-networks; Foreign, Commonwealth & Development Office, "Russia behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion," gov.uk, May 10, 2022, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion.
7 Pavel Polityuk and Stefaniia Bern, "Russian Attacks Leave Many Ukrainians without Power or Water," Reuters, October 31, 2022, https://www.reuters.com/world/europe/series-blasts-heard-kyiv-reuters-witnesses-2022-10-31/; Ievgeniia Sivorka, Reis Thebault, and Steve Hendrix, "Zelensky vows retribution after deadly Russian strike on Independence Day," *The Washington Post*, August 24, 2022, https://www.washingtonpost.com/world/2022/08/24/russia-ukraine-train-station-strike/.
8 Reuters, "Brace for Russian Cyber Attacks as Ukraine Crisis Deepens, Britain Says," January 28, 2022, https://www.reuters.com/world/europe/brace-russian-cyber-attacks-over-ukraine-britain-says-2022-01-28/; Cybersecurity and Infrastructure Security Agency, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," n.d., https://www.cisa.gov/uscert/ncas/alerts/aa22-011a.
9 Helene Cooper, "Russia and Ukraine Each Have Over 100,000 Casualties, Top US General Says," *The New York Times*, November 10, 2022,

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

https://www.nytimes.com/2022/11/10/world/europe/ukraine-russia-war-casualties-deaths.html.

[10] David Axe, "Ukraine Is Collecting A Lot of Russia's Old T-62 Tanks," Forbes, October 27, 2022, https://www.forbes.com/sites/davidaxe/2022/10/27/ukraine-is-collecting-a-lot-of-russias-old-t-62-tanks/?sh=2a4d991b30a5; General Staff of the Armed Forces of Ukraine (verified account), Facebook Infographic, October 22, 2022, https://www.facebook.com/photo.php?fbid=439777775001973&set=pb.100069092624537.-2207520000.&type=3.

[11] David Axe, "Ukraine Is Collecting A Lot of Russia's Old T-62 Tanks."

[12] Justin Bronk, "Is the Russian Air Force Actually Incapable of Complex Air Operations?," *RUSI Defence Systems* 24 (March 4, 2022), https://rusi.org/explore-our-research/publications/rusi-defence-systems/russian-air-force-actually-incapable-complex-air-operations; Sean M. Wismesser, "Potemkin on the Dnieper: the Failure of Russian Airpower in the Ukraine war," *Small Wars & Insurgencies* (March 29, 2023): 9–14, https://doi.org/10.1080/09592318.2023.2187201.

[13] Paul Iddon, "'Not Since World War II': The Worrying Precedent Many Are Evoking For The Ukraine War," Forbes, November 29, 2022, https://www.forbes.com/sites/pauliddon/2022/11/29/not-seen-since-world-war-ii-the-worrying-precedent-many-are-evoking-for-the-ukraine-war/?sh=2e66c1db76a3; Patrick Wintour, "Russia has amassed up to 190,000 troops on Ukraine borders, US warns," *The Guardian*, February 18, 2022, https://www.theguardian.com/world/2022/feb/18/russia-has-amassed-up-to-190000-troops-on-ukraine-borders-us-warns.

[14] Australian Cyber Security Centre, "Australian organisations encouraged to urgently adopt an enhanced cyber security posture," cyber.gov.au, February 23, 2022, https://www.cyber.gov.au/acsc/view-all-content/alerts/australian-organisations-encouraged-urgently-adopt-enhanced-cyber-security-posture; Canadian Centre for Cyber Security, "Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity," January 26, 2022, https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadian-critical-infrastructure-operators-raise.

[15] Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in an Age of Cyber Threats* (New York, NY: Penguin Press, 2019), 181–203.

[16] 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): 118–123, http://dx.doi.org/10.26153/tsw/42073.

[17] Martin Libicki, "The Cyber War That Wasn't," in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 50–54, https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf.

[18] Christopher Bronk, Gabriel Collins, and Dan Wallach, "Cyber and Information Warfare in Ukraine: What Do We Know Seven Months In?," Baker Institute for Public Policy, September 6, 2022, https://www.bakerinstitute.org/research/cyber-and-information-warfare-ukraine-what-do-we-know-seven-months.

[19] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, https://doi.org/10.1080/01402390.2011.608939; Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* 15 (2013): 105–122, https://doi.org/ 10.1111/misr.12023.

[20] John A. Gentry, "Intelligence Failure Reframed," *Political Science Quarterly* 123, no. 2 (Summer 2008): 247, https://www.jstor.org/stable/20203011.

[21] Gentry, "Intelligence Failure Reframed," 249.

[22] This definition is adapted from Roger Z. George, *Intelligence in the National Security Enterprise: An Introduction* (Washington, DC: Georgetown University Press, 2020), 7; Gentry, "Intelligence Failure Reframed," 247; Ehud Eiran, "The Three Tensions of

Investigating Intelligence Failures," *Intelligence and National Security* 31, no. 4 (2016): 602, https://doi.org/10.1080/02684527.2015.1044293, quoting Woodrow J. Kuhns, "Intelligence Failures: Forecasting and the Lessons of Epistemology," in Richard K. Betts and Thomas G. Mahnken (eds.), *Paradoxes of Strategic Intelligence: Essay in Honor of Michael I. Handel* (London, UK: Routledge, 2003), 81; John Hollister Hedley, "Learning from Intelligence Failures," *International Journal of Intelligence and Counterintelligence* 18, no. 3 (2005): 437, https://doi.org/10.1080/08850600590945416.

[23] Stephen Marrin, "Preventing Intelligence Failures by Learning from the Past," *International Journal of Intelligence and Counterintelligence* 17, no. 4 (2004): 657, https://doi.org/10.1080/08850600490496452.

[24] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (October 1978): 63, https://doi.org/10.2307/2009967; Gentry, "Intelligence Failure Reframed," 247.

[25] Eiran, "The Three Tensions of Investigating Intelligence Failures," 601.

[26] Eiran, "The Three Tensions of Investigating Intelligence Failures," 601.

[27] Gentry, "Intelligence Failure Reframed," 248.

[28] Mark A. Jensen, "Intelligence Failures: What Are They Really and What Do We Do About Them?," *Intelligence and National Security* 27, no. 2 (April 2012): 262, https://doi.org/10.1080/02684527.2012.661646.

[29] For an overview of the organizational pathologies that led to the intelligence failures around weapons of mass destruction (WMD) in Iraq; Richard K. Betts, "Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD," *Political Science Quarterly* 122, no. 4 (Winter 2007/2008): 585–606, https://www.jstor.org/stable/20202928.

[30] Betts, "Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD," 596–597.

[31] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (October 1978): 63, https://doi.org/10.2307/2009967.

[32] One of the more interesting works on this subject is Luis Garicano and Richard A. Posner, "Intelligence Failures: An Organizational Economics Perspective," *Journal of Economic Perspectives* 19, no. 4 (Fall 2005): 151–170, https://doi.org/10.1257/089533005775196723.

[33] Marrin, "Preventing Intelligence Failures by Learning from the Past," 655.

[34] Office of the Director of National Intelligence, "ODNI Factsheet," February 24, 2017, https://www.dni.gov/files/documents/FACTSHEET_ODNI_History_and_Background_2_24-17.pdf.

[35] Marrin, "Preventing Intelligence Failures by Learning from the Past," 656–658.

[36] Robert Jervis, "Reports, Politics, and Intelligence Failures: The Case of Iraq," *Journal of Strategic Studies* 29, no. 1 (February 2006): 10, https://doi.org/10.1080/01402390600566282.

[37] Gentry, "Intelligence Failure Reframed," 249.

[38] Austen Givens, "A Systems-Based Approach to Intelligence Reform," *Journal of Strategic Security* 5, no. 1 (Spring 2012): 65–66, http://dx.doi.org/10.5038/1944-0472.5.1.5.

[39] John Hollister Headley, "Learning from Intelligence Failures," *International Journal of Intelligence and Counterintelligence* 18, no. 3 (2005): 438–439, https://doi.org/10.1080/08850600590945416.

[40] Sherman Kent, "A Crucial Estimate Relived," *Studies in Intelligence* (1992), https://www.cia.gov/static/f547ed3bcd5793ff5456dc381c2df789/A-Crucial-Estimate-Relived.pdf: 9, italics in the original.

[41] Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston, MA: Little, Brown and Company, 1971), 68.

[42] Kent, "A Crucial Estimate Relived," 11.

[43] An example of this is the Office of the Director of National Intelligence's unclassified summary of the investigation into the origins of SARS-CoV-2, the virus which caused

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

the COVID-19 pandemic. While the unclassified summary does not contain information on intelligence sources and methods, its analyses and conclusions are understood to mirror those of the classified version of the document; Office of the Director of National Intelligence, Untitled Summary of COVID-19 Origin Investigation, https://www.dni.gov/files/ODNI/documents/assessments/Unclassified-Summary-of-Assessment-on-COVID-19-Origins.pdf.

[44] Michael Schwirtz and Scott Reinhard, "How Russia's Military Is Currently Positioned," *The New York Times*, November 20, 2022, https://www.nytimes.com/interactive/2022/01/07/world/europe/ukraine-maps.html; Reuters, "Russian troops now number 90,000 near Ukraine border after drills, Kyiv says," November 3, 2021, https://www.reuters.com/world/ukraine-says-russia-leaves-units-near-its-border-keeps-90000-troops-2021-11-03/.

[45] The Five Eyes Alliance was formed in the wake of World War II. It is arguably the most robust and formidable intelligence sharing agreement in the world. For an extended treatment of the Alliance; Corey Pfluke, "A history of the Five Eyes Alliance: Possibility for reform and additions," *Comparative Strategy* 38, no. 4 (2019): 302–315, https://doi.org/10.1080/01495933.2019.1633186.

[46] Reuters, "Brace for Russian Cyber Attacks as Ukraine Crisis Deepens, Britain Says," *U.S. News and World Report*, January 28, 2022, https://www.usnews.com/news/world/articles/2022-01-28/brace-for-russian-cyber-attacks-over-ukraine-britain-says.

[47] Cybersecurity and Infrastructure Security Agency, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," n.d., January 11, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-011a.

[48] Australian Cyber Security Centre, "Australian organisations encouraged to urgently adopt an enhanced cyber security posture," cyber.gov.au, February 23, 2022, https://www.cyber.gov.au/acsc/view-all-content/alerts/australian-organisations-encouraged-urgently-adopt-enhanced-cyber-security-posture; Canadian Centre for Cyber Security, "Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity,"; Cybersecurity and Infrastructure Security Agency, "NCSC-NZ Releases Advisory on Cyber Threats Related to Russia-Ukraine Tensions," February 18, 2022, https://www.cisa.gov/uscert/ncas/current-activity/2022/02/18/ncsc-nz-releases-advisory-cyber-threats-related-russia-ukraine.

[49] Cybersecurity and Infrastructure Security Agency, "Shields Up," n.d., https://www.cisa.gov/shields-up.

[50] Ellen Nakashima and Alex Horton, "Russian Government Hackers Have Likely Penetrated Critical Ukrainian Computer Systems, U.S. Says," *The Washington Post*, February 15, 2022, https://www.washingtonpost.com/national-security/2022/02/15/russia-ukraine-cyber-attacks/.

[51] Office of the Director of National intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, February 2022, https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Wstate-HainesA-20220308.pdf, 12.

[52] Lisa Ercolano, "Russia-Ukraine conflict maxes out cyberattack risk assessment index," Johns Hopkins University, *The Hub*, February 15, 2022, https://hub.jhu.edu/2022/02/15/russia-ukraine-maxes-out-cyber-attack-predictive-index/.

[53] Ercolano, "Russia-Ukraine conflict maxes out cyberattack risk assessment index."

[54] Stuart Madnick, "What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare," *Harvard Business Review,* March 7, 2022, https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare.

[55] Edward Segal, "Why the Impact of Russian Cyberattacks on Ukraine Could Be Felt Around the World," Forbes, February 23, 2022,

https://www.forbes.com/sites/edwardsegal/2022/02/23/the-impact-of-russian-cyberattacks-in-ukraine-could-be-felt-around-the-world/?sh=34167f3d56b2.

[56] Pavel Polityuk and Stefaniia Bern, "Russian Attacks Leave Many Ukrainians without Power or Water," Reuters, October 31, 2022, https://www.reuters.com/world/europe/series-blasts-heard-kyiv-reuters-witnesses-2022-10-31; Ievgeniia Sivorka, Reis Thebault, and Steve Hendrix, "Zelensky vows retribution after deadly Russian strike on Independence Day," *The Washington Post*, August 25, 2022, https://www.washingtonpost.com/world/2022/08/24/russia-ukraine-train-station-strike/.

[57] Timelines of events in this conflict independently assembled by Cynthia Brumfield at *CSO*, and by Accenture, a consultancy, were invaluable starting points for this section of the article. These timelines appear at Cynthia Brumfield, "Russia-linked cyberattacks on Ukraine: A timeline," *CSO*, August 24, 2022, https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html?page=3 and Accenture, *Global Incident Report: Russia-Ukraine Crisis*, April 21, 2022, https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/04/Global-incident-report-Russia-Ukraine-Crisis-April-21.pdf.

[58] Thomas Grove, "Russia's Draft Patched Holes but Also Exposed Flaws in War Machine," *The Wall Street Journal*, December 22, 2022, https://www.wsj.com/articles/russias-draft-patched-holes-but-also-exposed-flaws-in-war-machine-11671700783.

[59] Interfax-Ukraine, "Ukraine Sees Hacker Attack on Govt Websites at Night," January 14, 2022 https://en.interfax.com.ua/news/general/791472.html?mid=1#cid=241671.

[60] Microsoft, "Destructive Malware Targeting Ukrainian Organizations," February 8, 2022, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

[61] Microsoft, "Special report: Ukraine - an Overview of Russia's Cyberattack Activity in Ukraine," April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[62] Sean Lyngaas and Tim Lister, "Cyberattack Hits Websites of Ukraine Defense Ministry and Armed Forces," CNN, February 16, 2022, https://www.cnn.com/2022/02/15/world/ukraine-cyberattack-intl/index.html.

[63] Arne Welzel, Christian Rossow, and Herbert Bos, "On Measuring the Impact of DDoS Botnets," *EuroSec '14: Proceedings of the Seventh European Workshop on System Security* (April 2014): 4, https://doi.org/10.1145/2592791.2592794.

[64] White House, "Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh," February 18, 2022," https://www.whitehouse.gov/briefing-room/press-briefings/2022/02/18/press-briefing-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-and-deputy-national-security-advisor-for-international-economics-and-dep/.

[65] Microsoft, "Special report: Ukraine - an Overview of Russia's Cyberattack Activity in Ukraine," April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, 12.

[66] Microsoft Security Response Center, "Cyber threat activity in Ukraine: analysis and resources," February 28, 2022, https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/.

[67] Reuters, "Ukrainian Websites under 'nonstop' Attack - Cyber Watchdog Agency," March 5, 2022, https://www.reuters.com/world/europe/ukrainian-websites-under-nonstop-attack-cyber-watchdog-agency-2022-03-05/?mid=1#cid=753987.

[68] Joseph Cox, "Ukraine Arrests 'Hacker' It Says Was Routing Calls for Russian Troops," VICE Media, March 15, 2022, https://www.vice.com/en/article/v7djda/ukraine-arrests-hacker-routing-calls-for-russian-troops?mid=1#cid=838208.

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099

[69] Ben Nimmo, David Agronovich, Nathaniel Gleicher, "Adversarial Threat Report," Meta, April 2022, https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf: 17.
[70] Google Threat Analysis Group, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," February 2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf, 4.
[71] Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
[72] Microsoft, "Defending Ukraine: Early Lessons from the Cyber War," June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK: 8.
[73] Dan Goodin, "Mystery solved in destructive attack that knocked out > 10k Viasat modems," ArsTechnica, March 31, 2022, https://arstechnica.com/information-technology/2022/03/mystery-solved-in-destructive-attack-that-knocked-out-10k-viasat-modems/.
[74] Smith, "Defending Ukraine: Early Lessons from the Cyber War."
[75] State Service of Special Communications and Information Protection of Ukraine, "War in Ukraine: Pulse of Cyber Defense," July 2022, https://mcusercontent.com/95750673b8ed58984406ae56e/files/7d7f51a6-661f-a608-41ff-7f0828cb0e58/SSSCIP_Weekly_Digest_2022_07_ENG.pdf: 4.
[76] State Service of Special Communications and Information Protection of Ukraine, "War in Ukraine: Pulse of Cyber Defense," 5.
[77] Austen D. Givens, *Disaster Labs: How American States Use Partnerships to Manage the Unthinkable* (Quantico, VA: Marine Corps University Press, 2020), 87–91, https://doi.org/10.56686/9781732003101.
[78] Security Service of Ukraine, "SSU Shuts down Million-Strong Bot Farm That Destabilized Situation in Ukraine and Worked for One of Political Forces (Video)," August 2, 2022, https://ssu.gov.ua/en/novyny/sbu-likviduvala-milionnu-botofermu-yaka-rozkhytuvala-obstanovku-v-ukraini-na-zamovlennia-odniiei-z-politsyl-video.
[79] Google Threat Analysis Group, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," 6–8.
[80] Canadian Centre for Cyber Security, "Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine," June 2022, https://cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf: 3, Figure 1; Sana Noor Haq and Oleskandra Ochman, "Russia hits dam in central Ukraine, in latest attack on civilian infrastructure," CNN, September 15, 2022, https://www.cnn.com/2022/09/15/europe/russia-ukraine-kryvyi-rih-dam-strike-intl/index.html.
[81] The Economist, "Lessons from Russia's Cyber-War in Ukraine," December 1, 2022, https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine.
[82] Jeremy Fleming, "The head of GCHQ says Vladimir Putin is losing the information war in Ukraine," *The Economist*, August 18, 2022, https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine.
[83] The Economist, "Lessons from Russia's Cyber-War in Ukraine," December 1, 2022, https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine.
[84] Ukrainian Ministry of Science and Education, "Modern IT Education in Ukraine," 2019, https://mon.gov.ua/eng/osvita/visha-osvita/suchasna-it-osvita-v-ukrayini.
[85] Andrada Fiscutean, "Cybersecurity in wartime: how Ukraine's infosec community is coping," CSO, February 27, 2023, https://www.csoonline.com/article/3688360/cybersecurity-in-wartime-how-ukraines-infosec-community-is-coping.html.

[86] 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, Table 1.

[87] Sean Atkins, "A web of partnerships: Ukraine, operational collaboration, and effective national defense in cyberspace," The Atlantic Council, August 30, 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/a-web-of-partnerships-ukraine-operational-collaboration-and-effective-national-defense-in-cyberspace/; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[88] Canadian Centre for Cyber Security, "Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine," 2; Brad Smith, "Extending our vital technology support for Ukraine," Microsoft, November 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/.

[89] Foreign, Commonwealth & Development Office, "Russia behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion."

[90] Florian J. Egloff and Max Smeets, "Publicly attributing cyber attacks: a framework," *Journal of Strategic Studies* (March 2021): 1–32, https://doi.org/10.1080/01402390.2021.1895117.

[91] Microsoft, *Special Report: Ukraine, An Overview of Russia's cyberattack activity in Ukraine*, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd: 3.

[92] Dustin Volz, "Russia's War on Ukraine Deepens International Cyber-Defense Cooperation," *The Wall Street Journal*, September 6, 2022, https://www.wsj.com/articles/russias-war-on-ukraine-deepens-international-cyber-defense-cooperation-11662436289.

[93] AFP, "Moscow Says 100K IT Specialists Have Left Russia This Year," *The Moscow Times*, December 20, 2022, https://www.themoscowtimes.com/2022/12/20/moscow-says-100k-it-specialists-have-left-russia-this-year-a79754; Anthony Faiola, "Mass flight of tech workers turns Russian IT into another casualty of war," *The Washington Post*, May 1, 2022, https://www.washingtonpost.com/world/2022/05/01/russia-tech-exodus-ukraine-war/; Todd Prince, "'A Nail in the Coffin': Tech Workers Are Fleeing Russia and the Impact Will Last for Years," Radio Free Europe Radio Liberty, April 6, 2022, https://www.rferl.org/a/russia-it-workers-brain-drain/31783558.html.

[94] AFP, "Moscow Says 100K IT Specialists Have Left Russia This Year."

[95] One pre-print study about the Russian IT brain drain during the invasion of Ukraine is Johannes Wachs, "Digital Traces of Brain Drain: Developers during the Russian Invasion of Ukraine," September 2022, https://arxiv.org/pdf/2209.01041.pdf. The study has not yet been peer-reviewed.

[96] Wachs, "Digital Traces of Brain Drain: Developers during the Russian Invasion of Ukraine," 1.

[97] Erin Banco, Garrett M. Graff, Lara Seligman, Nahal Toosi, and Alexander Ward, "'Something Was Badly Wrong': When Washington Realized Russia Was Actually Invading Ukraine," POLITICO, February 24, 2023, https://www.politico.com/news/magazine/2023/02/24/russia-ukraine-war-oral-history-00083757; Greg Myre, "As Russia threatens Ukraine, the U.S. 'pre-bunks' Russian propaganda," NPR, February 8, 2022, https://www.npr.org/2022/02/08/1079213726/as-russia-threatens-ukraine-the-u-s-pre-bunks-russian-propaganda.

[98] Banco et al., "'Something Was Badly Wrong': When Washington Realized Russia Was Actually Invading Ukraine."

https://digitalcommons.usf.edu/jss/vol16/iss2/7
DOI: https://doi.org/10.5038/1944-0472.16.2.2099