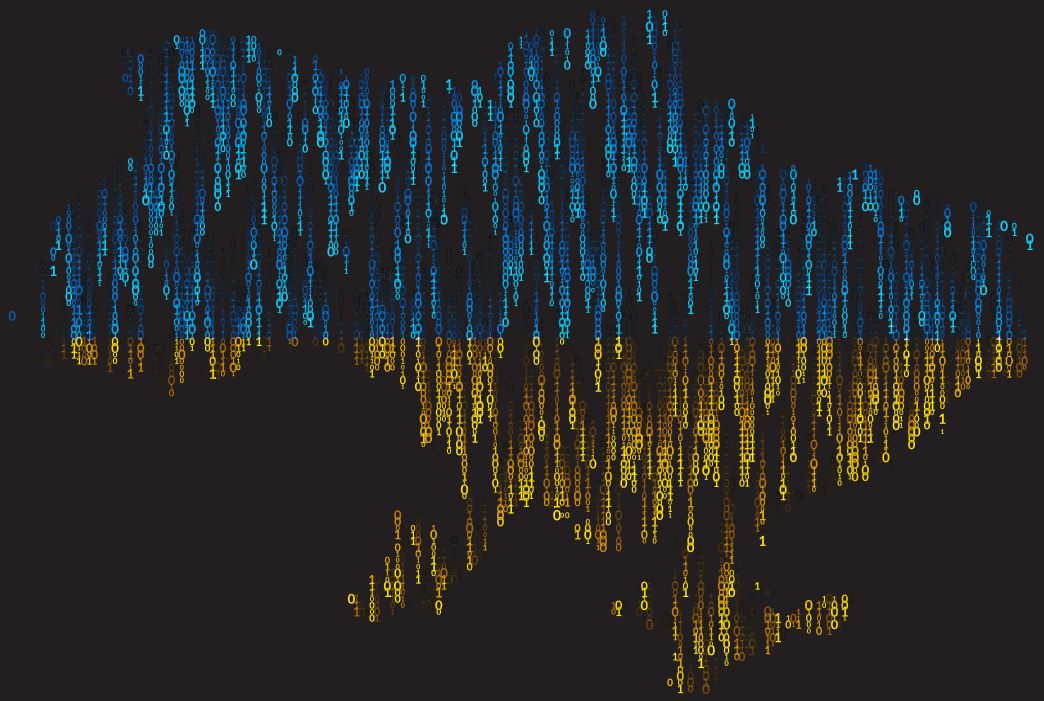

Unravelling the Myth of Cyberwar

Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)

Foreword by Volodymyr Shypovskyi

Per-Erik Nilsson

FOI-R--5513--SE

December 2023

FOI

Per-Erik Nilsson

Unravelling the Myth of Cyberwar

Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)

Foreword by Volodymyr Shypovskyi

Title	Unravelling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)
Report no	FOI-R--5513--SE
Month	December
Year	2023
Pages	86
ISSN	1650-1942
Client	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
roject no	E385091
Approved by	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Cover: Ukraine Digital Map Dots Particles Vector Stock Vector (Royalty Free) 2311399237 | Shutterstock.

Sammanfattning

Föreliggande rapport diskuterar varför Rysslands full-skaliga invasion av Ukraina inte har levt upp till mångas farhågor beträffande cyberkrigföring. I rapporten granskas fem huvudhypoteser som söker besvara denna fråga.

En första hypotes föreslår att ursprungliga förväntningar på Rysslands förmåga inom offensiv cyberkrigföring kan ha varit överdrivna. Detta kan ha lett till vilseledande bedömningar av situationen. Den andra hypotesen framhåller att Ryssland inte har utnyttjat sin fulla potential inom offensiv cyberkrigföring. Detta väcker frågor om hur deras faktiska kapacitet för denna typ av operationer ser ut. Hypotes tre ifrågasätter idén att rysk cyberkrigföring är ineffektiv. Istället betonas den betydande skada som redan har åsamkats, även om det inte utgör bevis för en omfattande cyberkrigföring. Den fjärde hypotesen föreslår att Ukrainas robusta cyberförsvar kan ha avskräckt en mer omfattande cyberkrigföring. Slutligen framhålls i den femte hypotesen att det som kan observeras är i linje med vad som kunde förväntas. En stor del av den tidigare forskningen på området har i över ett decennium påpekat att teorier om storskaliga cyberkrig kan leda teoretiker och beslutsfattare fel.

Rapporten understryker vidare vikten av att inte förhasta slutsatser kring någon enskild hypotes. Detta beror främst på att tillgängliga data ännu är ofullständiga. I rapporten betonas även vikten av att skilja mellan fientliga cyberoperationer under krigsförhållanden och de som sker inom en fientlig intrastatlig tävlan eftersom olika förmågor, juridiska och konceptuella ramverk är aktuella beroende på kontext.

Slutligen konstaterar rapporten att även om nuvarande bevis tyder på frånvaron av omfattande destruktiv cyberkrigföring, är rysk cyberkrigföring fortfarande en kraft att räkna med, särskilt som en möjliggörare av informationspåverkan och som komplement till militära kinetiska operationer. Framtida lärdomar bör därför bygga på gedigen empirisk evidens för att utveckla effektiva motåtgärder som omfattar tekniska, organisatoriska, samhälleliga och politiska aspekter baserade på faktiska förhållanden snarare än orealistiska framtidsbilder. Spekulativt tänkande är dock viktigt för att utforska framtida scenarier, men kan inte utgöra grunden för förståelsen av cyberkrigföring. Särskilt bör Ukrainas cyberförsvar och cybersäkerhetsarbete vidare utforskas. Detta kan säkerställa en realistisk och stark respons på det ständigt föränderliga landskapet av cyberhot i krig som i tider av ofred.

Nyckelord: cyber, krig, krigföring, strategi, försvar, Ukraina, Ryssland

Summary

This report delves into the ongoing Russo-Ukrainian war to discern whether it serves as a proof of concept for a large-scale cyberwar. Five prevailing hypotheses are examined to address this pivotal question.

The first hypothesis posits that initial expectations of Russian offensive cyber capabilities may have been exaggerated, potentially leading to misguided assessments. The second hypothesis contends that Russia might not have fully harnessed its potential for offensive cyber capabilities. The third hypothesis challenges the notion that Russian cyberwarfare is ineffectual, emphasising the considerable damage it has inflicted, even if not indicative of a full-scale cyberwar. The fourth hypothesis suggests that Ukraine's robust cyber-defence capabilities may have deterred a comprehensive cyberwar. Lastly, the fifth hypothesis posits that the very framing of the question of a cyberwar may be misleading, aligning with earlier research findings.

This report underscores the premature dismissal of any single hypothesis, primarily due to the incomplete nature of publicly available data. Additionally, it emphasises the critical need to differentiate between hostile cyber operations within the context of war and those within hostile intrastate competition or "unpeace." The report highlights the significance of establishing an analytical baseline rooted in empirically founded theory rather than speculative notions of an impending cyber apocalypse. While speculative thought is crucial for envisioning potential futures, it cannot serve as the bedrock of cyber theory.

Ultimately, this report concludes that although available evidence suggests the absence of a full-scale cyberwar, Russian cyberwarfare remains formidable and demands serious consideration. The lessons derived from this conflict should be grounded in solid empirical evidence, allowing for the development of effective countermeasures encompassing technical, organisational, societal, and political dimensions based on empirical realities rather than unrealistic futuristic scenarios. This approach ensures a pragmatic and robust response to the evolving landscape of cyber threats.

Keywords: Cyber, War, Warfare, Strategy, Defence, Russia, Ukraine

Contents

Acknowledgements

This report stands as a testament to the collective wisdom and support extended by a remarkable group of individuals, to whom I owe a great debt of gratitude. Their keen eyes and astute minds have left an indelible mark on the report.

In particular, I extend my heartfelt thanks, in alphabetical order, to Sarah Backman, Patrik Fältström, Mattias Hansson, Richard Langlais, Volodymyr Shypovskyi, Mattias Svahn, Carolina Vendil Pallin, Mikael Wedlin, and Pontus Winther. Their perspectives and feedback have not only enhanced the quality of this work but also my own understanding of the subject.

While this report is a collaborative effort, I shoulder the responsibility for any errors that may remain.

Per-Erik Nilsson, Kista

2023-12-09

Executive Summary

This report aims to comprehensively understand cyberwarfare's role in the Russo-Ukrainian war. What can be concluded and learned re-garding the cyberwarfare we are seeing there?

Chapter 2, "What about Cyber?", discusses theoretical approaches to cyberwar and cyberwarfare. The chapter's key takeaways are:

- Cyberspace encompasses all computer networks and connections, extending beyond the internet to include diverse networks not accessible to the public. There is an ongoing scholarly debate about whether cyberspace should be considered a distinct domain of warfare alongside land, sea, air, and space, due to its increasing integration with other domains, driven by technological advancements. This report argues that *cyberspace* pertains to data and technical infrastructure, while the *cyber domain* encompasses social, political, and legal dynamics.
- Distinguishing between "cyberwar" and "cyberwarfare" is crucial, with the latter providing a more precise description if one considers its relevance within armed-conflict scenarios and acknowledges the need for physical force.
- The term "unpeace" recognises the evolving dynamics of cyberspace, where offensive cyber operations, enabled by increased connectivity and digitalisation, expose new vulnerabilities, expanding the role of cyberspace in conflicts. This is particularly relevant to the Russo-Ukrainian war, which has led states to find themselves in a condition of "unpeace" in their interactions with Russia, even though they are not outright war, as Ukraine's are.
- An attempt to construct a clear hierarchy to categorise the sometimes ambiguous connection between cyberattacks and exploits is introduced. This hierarchy includes, in descending order, cyber campaigns, cyber operations, cyber exploits, and cyberattacks, each building upon the other in terms of complexity and impact.

Chapter 3, "Russia's Hostile Cyber Activities in Ukraine," discusses publicly available accounts and interpretations of Russian cyber campaigns and cyber operations conducted in Ukraine between 2014 and 2023.

- Russia's cyber activities between 2014 and 2022 exhibited a spectrum of sophistication, from basic to advanced operations, yet they did not reach the level of the catastrophic. Several scholars contend that the activities recorded, except for NotPetya, had negligible strategic value. However, few support the strategic value of Russia's cyber-enabled information campaign for the annexation of Crimea, which focused on informational con-

trol and provoked distrust among the population. Offensive cyber operations before the full-scale invasion in 2022 were of limited scope, leading some scholars to conclude that it was mainly an example of vandalism rather than the full potential of cyberwarfare.

- The numerous campaigns and operations in 2022 and 2023 should be viewed as more than mere cyber vandalism. Based on available data, the potential strategic value of cyber operations in multidomain operations is uncertain. While there is a correlation between cyber and kinetic operations, causation is not established. Given the lack of cataclysmic impact, the discussion considers whether cyberwarfare is best understood as a force multiplier in shaping the battlefield rather than a large-scale "cybergeddon."
- That Russian APT actors likely increased their access to Ukrainian military networks and soldiers' devices demonstrates the potent usage of cyber operations in war.

Chapter 4, "What Happened to the Cyberwar?" discusses the first four central hypotheses for explaining the role of hostile Russian cyber activities during the war:

- The *Wrong Expectations Hypothesis* suggests that an overly optimistic assessment of Russian cyber capabilities, which may not have been realised as anticipated, may also have led to disappointment in the actual cyberwarfare outcomes.
- The *Failed Capabilities Hypothesis* contends that Russia's offensive cyber capabilities may have suffered due to strategic and tactical misdirection, inadequate planning, and a lack of strategic transparency.
- The *Failed Analysis Hypothesis* argues that Russia's cyber operations, including coordinated cyber and kinetic campaigns, have historically had a significant impact and still do. Moreover, Russia came close to capturing Kyiv, prompting a potential contrafactual reevaluation of perceptions of Russian cyber capabilities. Also, Ukraine's increasing adoption of sophisticated technologies may create additional vulnerabilities to cyber operations, highlighting the dynamic nature of cyberwarfare.
- The *Successful Defence Hypothesis* focuses on Ukraine's ability to withstand cyber onslaughts, which relies on three key pillars. The first is experience accumulated from nearly a decade of being targeted by Russian cyber operations. The second is international support, in terms of resources and expertise in cyber defence and overall security. The final one, which is speculative, is that successful counteroffensive cyber campaigns have been debilitating Russia's offensive capabilities, thus strengthening Ukraine's defensive posture.
- The chapter's overall assessment suggests that it is premature to entirely dismiss any of these hypotheses, given the evolving nature of cyberwarfare. However, the *successful defence hypothesis* holds particular weight, regardless of the validity of the other propositions. In addition, establishing

baseline measurements and ensuring that data is reliable are critical in assessing the true extent of Russia's cyber capabilities, although accessing that data is accurate and comprehensive, especially for external observers, poses a challenge.

Chapter 5, "Adjusted Expectations," discusses the hypothesis of "adjusted expectations." This hypothesis suggests that the extent of Russia's cyber activities aligns with what can be reasonably anticipated based on empirical evidence and theoretical knowledge. The core of the hypothesis is:

- Constraints on the effectiveness of cyberattacks, including the need for discernible strategic intent and the "trilemma" of speed, intensity, and control, are significant factors in evaluating cyberwarfare. The human element adds complexity to cyber operations, requiring seamless coordination and resource allocation.
- The Russo-Ukrainian war is not a definitive proof of concept for full-scale cyberwar, but this does not diminish the significance of cyberwarfare in contemporary conflicts. While cyber operations may not serve as the sole determinant of interstate war, they act as a force multiplier, broadening the dimensions of warfare.
- Lessons learned from current cyber activities should be approached cautiously, and theoretical insights applied judiciously. Recognising that countries other than Ukraine may have varying levels of resilience to hostile cyber activities is vital.
- Downplaying the threat of cyberwarfare would be a severe mistake, emphasising the need for vigilance in cyberspace.

Foreword

By Volodymyr Shypovskyi, National Defence University of Ukraine

"In the end, all attacks are against the human element, not the technology."

Amit Yoran

In the ever-evolving landscape of contemporary warfare, the relentless ascent of information technologies has rendered warfare increasingly complex. This transformation has, in turn, catalysed a constant cycle of technical innovations during wars, yielding novel tools and methods for countermeasures. Within this shifting paradigm, the cyber domain has emerged as an indispensable and dynamic part of the theatre of war, altering the nature of multidomain conflicts. Against this background, the focus of this comprehensive report is to meticulously dissect the intricate specifics of the Russian Federation's utilisation of the cyber domain against Ukraine. By doing so, the report unravels the multilayered tapestry of modern cyberwarfare, considering its various dimensions, implications, and consequences.

Since Russia's full-scale invasion, in February 2022, we have witnessed several innovations in the conduct of war, when unmanned vessels in the air, on land, and in the sea have overturned past laws of intelligence and the conduct of battle at the tactical and operational levels. However, the Russo-Ukrainian war has not turned into a Hollywood sci-fi struggle between automated robotic systems. As in preceding wars, tanks are ablaze, soldiers are perishing, and Ukrainian civilians are succumbing. However, information technology has altered the contours of war and will continue to do so. Military doctrines and rules of warfare were written yesterday; they should be changed according to today's and future challenges.

The confluence of information technologies and warfare has not only altered the weapons at our disposal but has also blurred the lines between the physical and the virtual realms. Once dominated by tanks, aircraft, and infantry, traditional military arsenals have been supplemented with a formidable array of cyber capabilities. These capabilities extend into the digital domain, capable of infiltrating and disrupting information systems, critical infrastructure, and even the very fabric of society itself. As we embark on a journey to explore the nuances of Russia's cyber activities against Ukraine, it becomes evident that the cyber domain is no longer an isolated entity but a seamlessly integrated part of the broader theatre of multidomain conflicts.

The origin of this multidomain war is a result of the prolonged hybrid threat from the Russian Federation against Ukraine that has been escalating since 2014 (when

Russia annexed Crimea). The hybrid threat, characterised by a combination of conventional military tactics, cyberattacks, disinformation campaigns, and irregular warfare, has been a deliberate and evolving strategy used against Ukraine. This combination of tactics has created a complex and adaptive security environment in which destructive activities in the cyber domain operate in synergy with more traditional kinetic operations, as evidenced by the start of Russia's large-scale invasion. Such synergies between domains underscore the complexity of modern conflicts and the importance of an integrated and comprehensive approach to national defence.

One particular aspect of cyberwarfare in the Russo-Ukrainian war is the unpredictability of its consequences. The actions of special units within the Russian Federation's cyber capabilities have often led to outcomes significantly different from their initial plans. These unanticipated and sometimes far-reaching consequences have posed unique challenges for Russia's cyber strategy, prompting adjustments and changes during the ongoing war. Within this ever-shifting landscape, we can discern the intricacies of cyberwarfare strategies and their real-world implications. Understanding these dynamics is essential for comprehending the evolving nature of modern warfare.

Russia boasts formidable cyber capabilities supported and funded by its government. With a sophisticated arsenal, extensive resources, and a workforce skilled in cyber operations, these cyber forces have orchestrated diverse operations against Ukraine. These operations encompass disinformation campaigns, critical infrastructure attacks, and the continuous development of advanced cyber tools and techniques. However, despite these formidable threats, Ukraine has demonstrated remarkable resilience in countering the insidious attacks launched by Russian cyber troops. This resilience is a testament to Ukraine's dedication to bolstering its cyber defence and the vigilance of its cybersecurity experts.

In the face of such formidable and ever-evolving threats, the importance of cooperation cannot be overstated. Cyber defence is not the sole responsibility of the military; it necessitates active collaboration between the public sector, civil society, the military, and society at large. This multifaceted cooperation is pivotal in fortifying a nation's cyber defences and responding effectively to cyber threats. It highlights the essential role of collective security in the digital age, where the boundaries between government, the private sector, and civil society blur and resilience is a collective endeavour. A critical factor in the success (at the time of writing) was the assistance to Ukraine from partner states and individual specialists in cyber security, who independently united in groups and showed that justice has power and most countries support Ukraine in all dimensions, even cyber.

This report aspires to provide a comprehensive analysis of the intricate dynamics of cyberwarfare, focusing on the Russian Federation's cyber operations against Ukraine. By delving deep into the evolving nature of cyber threats, the innovative

countermeasures born in the crucible of conflict, and the critical role of cooperation in defending the state against cyber onslaughts, it seeks to unravel the complex interplay between technology, strategy, and resilience in the realm of modern cyberwarfare. In doing so, it aims to shed light on the broader implications for international security, defence strategies, and the evolving nature of modern warfare in the digital age.

In contemporary military conflicts, pinpointing the exact locations of combat operations has become an elusive endeavour, as these theatres of engagement are unbound by traditional geographical constraints. While there is cyberwarfare conducted against Ukraine, global security becomes more complex and challenging, so that the comprehensive analysis presented here is a welcome contribution to understanding what everyone is up against.

Kyiv, 10 October 2023

1 Introduction

In the spring of 2021, social media users and journalists started publishing satellite images of the Russian Armed Forces moving troops closer and closer to the Ukrainian border.1 The essay by Russian President Vladimir Putin, "On the Historical Unity of Russians and Ukrainians," published in July the same year, added fuel to the speculation about the Kremlin's real intentions with the military buildup on the Russian-Ukrainian border.[2]

In the following months, speculations about a potential Russian offensive increased in the news media. In social media, amateur open-source intelligence accounts were filled with images and videos of advanced Russian mobilisation. In early winter, US Secretary of State Anthony Blinken stated that there was "evidence that Russia has made plans for significant aggressive moves against Ukraine."[3] On 24 February 2022, Blinken's warning became reality.[4]

During the Russian buildup and the initial phase of the full-scale invasion, many academics and other experts published think pieces on the role that "cyber" would potentially play in the event of a full-scale invasion. Keir Giles, a renowned expert on Russian security policy and Senior Fellow at Chatham House, wrote that a "destructive cyber onslaught" potentially "could target military command and control

[1] See, for example, "Satellite Images Show Military Buildup in Russia, Ukraine," Radio Free Europe and Radio Liberty, 21 April 2021: https://www.rferl.org/a/russia-ukraine-military-buildup-satellite-images/31214867.html; Michael Gordon and Georgi Kantchev, "Satellite Images Show Russia's Expanding Ukraine Buildup," *Washington Post*, 20 April 2021: https://www.wsj.com/articles/satellite-images-show-russias-expanding-ukraine-buildup-11618917238.

[2] The essay is an exposé of allegedly essential historical, cultural, and religious ties between Russians and Ukrainians. However, the essay argues that since the Euromaidan in 2013–2014, Ukraine has gone astray from its real essential identity. Moreover, it states that "true sovereignty of Ukraine is possible only in partnership with Russia." See Vladimir Putin, "On the Historical Unity of Russians and Ukrainians," *President of Russia*, 12 July 2021: http://en.kremlin.ru/events/president/news/66181.

[3] Anthony Blinken in: Shane Harris and Paul Stone, "Russia Planning Massive Military Offensive against Ukraine Involving 175,000 Troops, US Intelligence Warns," *Washington Post*, 2 December 2021: https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

[4] While leaders of many Western countries were surprised by the scale of the invasion, in an interview after the full-scale invasion, the chief of the Ukrainian Military Intelligence Service (SBU) stated that he had already expected the invasion as early as in the spring of 2021. See interview with Kyrylo Budanov in: Dmitriy Komarov, "Рік - Частина четверта [Year – Part Four]," *Світ навиворіт* [The World Inside Out], 19 May, 2023: https://www.youtube.com/watch?v=yaOE1SDvJ6A.

systems or civilian critical infrastructure and pressure Kyiv into concessions and its friends abroad into meeting Russia's demands."[5]

In Recorded Future News, it was reported that a senior official of the Biden Administration had stated that "Russia could opt to launch a sweeping cyber and disinformation campaign against Ukraine and its government rather than a traditional military invasion of the country."[6]

William Courtney and Peter A. Wilson, of the Rand Corporation, pondered whether, if "Russia were to invade Ukraine, it would likely employ massive cyber and electronic warfare tools and long-range PGMs [precision-guided munition]" and continued to state that "the aim would be to create 'shock and awe,' causing Ukraine's defences or will to fight to collapse."[7]

Statements of this sort tap into long-ranging debates about the potential of cyberwarfare.[8] At its most elevated estimations, this potential has been equated to "A Cyber Pearl Harbour," or a Hollywood-style Armageddon, a "cybergeddon."[9] Given that Russia, which before the full-scale invasion was by many perceived as the most significant military power next to the USA, was also considered to possess an infamous cyberwarfare capability, expectations about the realisation of cyberwarfare's full potential were plenty: Was this the moment when the world would see the first large-scale cyberwar?

By all accounts, Russia's full-scale invasion of Ukraine at the time of writing had failed to live up to these expectations. This war is not proof of the concepts of a full-scale "cyberwar," "Cyber Pearl Harbour," or "cybergeddon," nor does Russia seem to have achieved any significant strategic effect with its cyberwarfare, either

---

[5] Keir Giles, "Putin Does not Need to Invade Ukraine to Get His Way," *Chatham House*, 21 December 2021: https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.

[6] Martin Matishak, "Russia Could Launch Digital Offensive Against Ukraine, Administration Official Warns," *The Record: Recorded Future News*, 6 December 2021: https://therecord.media/russia-could-launch-digital-offensive-against-ukraine-administration-official-warns.

[7] William Courtney and Peter A Wilson, "If Russia Invaded Ukraine," *The Rand Blog*, 8 December 2021: https://www.rand.org/blog/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html.

[8] For a discussion about the different perspectives on cyberwarfare and a potential cyberwar, see Sarah Backman, *Making Sense of Large-scale Cyber Incidents: International Cybersecurity Beyond Threat-based Security Perspectives* (Stockholm: Stockholm University, 2023), p 7–11.

[9] Leon Panetta, former United States Secretary of Defense (2011–2013) and Director of the CIA (2009–2011), famously warned in 2012 of our facing a potential "Cyber Pearl Harbor," a statement he has double-downed on since. See Jeff Erickson, "The Possibility Of A Cyber Pearl Harbor Remains Real, Says Former CIA Director," *Forbes*, 13 March 2019: https://www.forbes.com/sites/oracle/2019/03/13/the-possibility-of-a-cyber-pearl-harbor-remains-real-says-former-cia-director/?sh=5a46a50859fb.

on the battlefield or politically. Ciaran Martin, the former CEO of the UK's National Cybersecurity Centre is quoted to have concluded that the "idea that war was moving online primarily, which has been put around for a quarter of a century," simply "is not accurate."[10]

However, the explanations for the absence of the supposed full potential of cyberwarfare and the Russian strategic effect through cyberwarfare differ. Some argue that the reason for this absence needs to be directed to expectations of Russian cyberwarfare capabilities. Others suggest that the lack is due to Russia's failure to reach its full potential. Another set of arguments holds that Russia is not performing as poorly as is often claimed. Other statements claim that the absence is primarily because of a solid Ukrainian defensive capability. Finally, while other explanations focus on misdirected expectations of Russian cyberwarfare capabilities, they concede that the observed effect of Russian cyberwarfare, in theory and practice, is exactly what is to be expected, based on adjusted earlier analysis and scholarship.

1.1 Purpose

This report has been produced for the Swedish Armed Forces (SAF) as part of the Research and Organisation Development (FoT) with the Swedish Defence Research Agency (FOI). As such, this report directly responds to the SAF's mandate to address cyberwarfare at a strategic level, focusing on its implications in security politics. Recognising the global relevance and the need for international engagement and cooperation, the report is presented in English rather than Swedish.

Setting out from this premiss, the report aims to create an overall understanding of the role of cyberwarfare in the Russo-Ukrainian war. It seeks to answer the question of what conclusions can be drawn about cyberwarfare from this war. The present author has no illusions of originality. Many referenced articles and reports discuss the same topic from similar perspectives.[11] The ambition of this report, however, is to contribute to this ongoing debate.

---

[10] Martin in: Maggie Miller, "The World Holds Its Breath for Putin's Cyberwar," *Politico*, 23 March 2022: https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440.

[11] See, in particular, Joe Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Working Paper, Carnegie Endowment for International Peace, Washington, 2022, p 7: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657; Gavin Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations," Working Paper, Carnegie Endowment for International Peace, Washington, 2022: https://carnegieendowment.org/files/202212-Wilde_RussiaHypotheses-v2.pdf.

This is achieved by assessing and discussing five hypotheses regarding the lack of Russian strategic effect in cyberwarfare to date: a) wrong expectations; b) failed capabilities; c) failed analysis; d) successful defence; e) adjusted expectations.

The intended readers of this report are first of all, the SAF's personnel (e.g. FST STRA CYBER), but also policymakers and practitioners, analysts and researchers, and anyone interested in the report's topic. For this reason, the report explains basic concepts and provides references for further reading.

1.2 Data and Method

This report is a literature study of explanations of the role played by cyberwarfare in the Russo-Ukrainian war, from its start in 2014, with the invasion of Crimea and Eastern Ukraine, to Russia's full-scale invasion, in early 2022.

The analysed material consists of policy papers and reports, academic articles, and editorial material in the news media and magazines published by renowned research institutes, think tanks, scholars, analysts, and journalists. The main selection criteria was that the literature had been published since Russia's full-scale invasion of Ukraine. The literature was identified by searching through the publications of renowned research institutes and think tanks, academic databases, and news media and magazines.

In terms of method, the literature was systematically read and grouped into the five above-mentioned hypotheses that attempt to explain how to interpret the cyberwarfare observed as part of the larger war (see Section 1.1).[12]

The sections on cyberattack refer to publicly available data compiled by the Cyber Peace Institute, reports from cyber-security actors, such as Microsoft, Google, and Recorded Future, and the public accounts of cyberwarfare practitioners and strategists.

To assess and discuss the hypotheses, this report draws on the research literature on cyberwarfare, mainly involving the intersections of data science, international relations, and security studies.

One central methodological issue must be addressed when evaluating compiled data on hostile cyber activities: analysts and scholars rely on conceptually different understandings when classifying hostile cyber activities, cyber campaigns, cyber

[12] More specifically, the method is a simple form of Weberian ideal-type analysis, based in a critical realist epistemology. This means that the author of the report has construed these hypotheses from the body of literature used as empirical material. For further reading on methodology, see Emily Stapley, Sally O'Keeffe, and Nick Midgley, "Developing Typologies in Qualitative Research: The Use of Ideal-Type Analysis," *International Journal of Qualitative Methods* 21, online first (2022): 1–9.

operations, and cyberattacks. For example, some analysts classify operations, exploits, and cyber-enabled information warfare in a single general category, as attacks, while others distinguish between them. Since it is beyond the scope of this report to examine the methodological choices made by secondary sources and reinterpret their analyses, Chapter Two addresses this limitation by devoting more space to a thorough discussion of the conceptual understanding that this report applies to the phenomenon of hostile cyber-activity.

1.3 Limitations

There are three significant limitations to this report. The first one concerns the selection of literature for the analysis. Since this report concerns ongoing war, new accounts on the topic are continuously published, and some late discoveries of earlier publications have not been included in the analysis. For this reason, it is a likely assumption that the report's author has failed to address several other hypotheses.

The second limitation is a general caveat regarding data in cyberwarfare research. Cyber intrusions frequently result in implications involving magnitudes of 10,000 or 100,000 instances. Reporting on cybercrime in 2022, the American Federal Bureau of Investigation's (FBI) Crime Complaint Center (IC3) reported 800,944 complaints.[13] In France, a Senate Report investigating the impact of cybercrime on the private sector reports that 43% of French small and middle-size companies (PMEs, *petites et moyennes entreprises*) had been targeted in 2020.[14] Meanwhile, as there is an overflow of data on cyber incidents, it is difficult for the external observer to distinguish the clutter from actual threats. Moreover, many incidents are not reported, for security reasons, making it even harder for an external observer to validate the data. Coupled with preconceived notions of cyberwarfare and its relevance for security and international politics, research on cyberwarfare risks being biased regarding epistemology and data selection. As Lucas Kello states:

> The observable realm of cyber incidents, while varied and rich, does not reveal the full scope of real action, because of the many obstacles of data security… in building datasets on observable cases, the invocation of potentially outmoded concepts of interstate violence and conquests may lead thinkers to ignore nontraditional but relevant incidents and actors… sometimes

[13] "Internet Crime Report Center Releases 2022 Statistics," *Federal Bureau of Investigation,* Springfield, 22 March 2023: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics.

[14] See Sébastien Meurant and Rémi Cardon, *Rapport d'information fait au nom de la délégation aux entreprises relatif à la cybersécurité des entreprises*, Report no 678, The French Senat, 10 June 2021: https://www.senat.fr/rap/r20-678/r20-6781.pdf.

> the most important events in theory construction are those that did not occur but may plausibly happen.[15]

Somewhat provocatively, Kello suggests that "there is perhaps no other domain of security in which researchers know so little about so much activity."[16]

The third limitation concerns the second limitation in the context of the Russian-Ukrainian war. At the time of writing, the publicly available data identified for this report mainly concerns attacks on civilian and not military targets, making it difficult to assess the impact of cyber operations on the battlefield. Officials from Ukraine have also declared that they do not share data on all incidents,[17] as they should not. Writing about the issue of incident reporting, Nicholas Michael Sambaluk notes that "[s]uccessful defenders are wise not to crow too loudly about their successes, since an attacker has to be right once in a way that a defender has to be right each time," and adds that "failed attacks are far more easily hidden from a global public than can be the case with compromised defence."[18]

Similarly, in evaluating reports issued by private cybersecurity firms, it is imperative to exercise a critical perspective, particularly regarding the potential biases inherent in their assessments. Companies driven by commercial imperatives may possess financial interests that could inadvertently influence their portrayal of cyber threats. Consequently, they might amplify specific threats, aligning with their business objectives while minimising others. This dynamic necessitates a cautious approach to interpreting their findings, ensuring that the analysis of cyber threats remains grounded in comprehensive evidence rather than influenced by the vested interests of these entities.[19]

---

[15] Lucas Kello, *The Virtual Weapon and International Order* (New Haven and London: Yale University Press, 2018), p 11.

[16] Kello, *The Virtual*, p 41.

[17] See, for example, Illia Vitiuk (Head of the Department of Cyber and Information Security of the Security Service of Ukraine (SBU), interviewed in: Dmitri Alperovich and Patrick Gray, "How Russian Intelligence Operatives Have Attacked Ukraine in Cyberspace: Interview with the Security Service," *Geopolitics Decanted*, 21 August 2023.

[18] Nicholas Michael Sambaluk, *Myths and Realities of Cyber Warfare: Conflict in the Digital Realm* (Santa Barbara: Praeger Security, 2020), p 59.

[19] See Bateman, "Russia's Wartime," p 7: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657; Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal* 3 (2011): 1-39; Lennart Maschmeyer, Ronald J. Deibert, and Jon R. Lindsay, "A Tale of Two Cybers - How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society," *Journal of Information Technology & Politics* 18, no 1 (2021): 1–20.

Moreover, as described by the authors of a RUSI report on the first six months of conventional warfare during the full-scale invasion, a "great many definitive statements have been made about Russian capabilities based on the propaganda material produced by both sides," adding that there is, "therefore, a high risk that false lessons will be drawn from the war."[20]

Given these caveats, an external observer should tread lightly in evaluating cyberwarfare theory based on this case when drawing conclusions and suggesting the lessons learned. To quote Herbert Lin: "[C]onclusions regarding the importance of cyber operations to the conduct of the Russian-Ukraine war are preliminary at best, and generalisations about the strategic utility of offensive cyber operations for coercion are almost certainly premature."[21]

1.4 Disposition

The following chapter (Chapter Two) presents an overview of academic theory on cyberwarfare and related concepts, i.e., cyberwar, cyber operations, cyberattacks, cyberspace, and the cyber domain. These concepts are moreover discussed regarding their relevance for the analysis of cyberwarfare concerning the Russo-Ukrainian war. Chapter Three provides an overview of publicly available data on Russian cyberattacks in Ukraine since 2014, focusing on the period after the full-scale invasion, in 2022. Chapter Four presents and discusses the first four hypotheses on the absence of strategic effects from cyberwarfare. These hypotheses explicitly concern Russia's and Ukraine's offensive and defensive cyber capabilities. In Chapter Five, these four hypotheses are discussed in relation to the fifth, a metatheoretical hypothesis about the nature of cyberwarfare. The concluding chapter provides preliminary suggestions on the war's implications for cyber theory and an identification of focus areas for future lessons learned.

[20] Mykhaylo Zabrodskyi, Jack Watling, Oleksandr Danylyuk V, and Nick Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*, Royal United Services Institute for Defence and Security Studies (RUSI), London, 2022, p 4: https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

[21] Herbert Lin, "Russian Cyber Operations in the Invasion of Ukraine," *The Cyber Defence Review* 7, no. 4 (2022): 31–45, p 42.

2 What about "Cyber"?

Linguistically, cyber is both an adjective and a combining form that, at its most basic, refers to something "relating to, or involving computers or computer networks (such as the internet)."[22] As such, it has come to be attached to various phenomena: cyberwar, cyberwarfare, cyberterrorism, cyber operations, cyberattacks, cybercrime, cyber intrusions, cyber defence, cyber security, cyberweapons, and cyber vulnerabilities. It also denotes a broad range of actors: cyber soldiers, cyber defenders, cybercriminals, cyberterrorists, cyberpolice, cybervictims, cyberbullies, hackers, and crackers.

Given the advent of the internet and the digitalisation of virtually all aspects of human life, these lists could be far longer. This historically new integration of digital networks with human life has given rise to conceptualisations that allow us to understand this intersection. Cyberspace or the cyber domain are often used interchangeably to denote this networked virtual and physical intersection. This intersection does not exist in a vacuum.[23] It is embedded in technology and social, political, and economic relations, affecting how humans perceive and live their lives. "Cyber" is everywhere, but without clear definitions of what "cyber" means, it runs the risk of being nowhere, as an unobservable background noise.

Against this background, this chapter aims to clarify how central "cyber" concepts are understood and used in this report.

2.1 Cyberspace and the Cyber Domain

Scholars and policymakers, both civilian and military, have been discussing how to define and delineate cyberspace since the 1990s. This report defines cyberspace as all existing computer networks, connections, and means of control.[24] As Richard A Clarke and Robert K Knake remind us, cyberspace is thus more than the internet, since it includes the internet, "plus lots of other networks of computers that are not supposed to be accessible from the Internet."[25] This means that cyberspace has virtual (digitally stored data and traffic through cables and radio waves)

[22] Merrian-Webster, "Cyber," 27 August 2023: https://www.merriam-webster.com/dictionary/cyber.

[23] For a discussion on the social, political, economic, and cultural embeddedness of "cyber," see David Holmes, "Virtual Politics – Identity and Community in Cyberspace," in *Virtual Politics: Identity and Community in Cyberspace*, ed David Holmes (London, Thousand Oaks, and New Delhi: Sage Publications, 1997), 1–24.

[24] See Richard A Clarke and Robert K Knake, *Cyber War: The Next Threat to National Security, and What to Do About It* (New York: HarperCollins, 2010), p 69; Christopher Whyte and Brian Mazanec, *Understanding Cyber-Warfare: Politics, Policy, and Strategy* (London and New York: Routledge, 2021), p 31–32.

[25] Clarke and Knake, *Cyber War*, p 69.

and physical (computers, microchips, servers, cables, routers, and so on) dimensions.

A closely related question to the conceptualisation of cyberspace is whether it is a distinct warfighting domain, the fifth domain. The other domains are land, sea, air, and space. There is a whole conceptual debate around this issue that is not the topic of this report; regardless of whether it is seen as a separate domain or not, it is typically stated that the cyber domain is the first human-made domain. This means that cyberspace is different from the other domains. Even if land can arguably be seen as partially artificial (cities and geo-engineering), new technology changes human capacity to travel on the sea, in the air, and space; gravity, geography, and time make these domains relatively constant. However, cyberspace pertains to other sets of rules. The terrain itself is plastic and, given rapid technological developments, constantly developing, not only in the tools humans use to exploit the landscape, but also in the way their tools in turn transform it.[26]

Some argue, thus, that conceptualising cyberspace as a separate domain of warfighting is a fault, not least since it is increasingly integrative with the other domains.[27] Another approach to the question of the domain status of cyberspace is Kello's proposal to conceptualise the cyber domain as "the bevy of human and institutional actors that operates and regulates cyberspace itself."[28]

Drawing on Kello, and for the sake of clarity, cyberspace is understood here as the technical plane, while the cyber *domain* is seen as the human, social and political plane. What is not at issue, then, is the degree to which cyberspace should be seen as a separate warfighting domain.[29] Notwithstanding those aspects, however, cyberspace is also understood here as an increasingly integrative part of the other domains.

---

[26] Sambaluk, *Myths and Realities*, p 34.

[27] See Martin Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no 2 (2012): 321-36; Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal: Canada's Journal of Global Policy Analysis* 69, no 3 (2014): 394-412; Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare* (London, Hurst & Company, 2022), p 46. It should be noted that there are bureaucratic benefits of recognizing cyber as a unique domain, since it brings about visibility and impact on resource allocation and structural organization within security frameworks.

[28] Kello, *The Virtual Weapon*, p 46.

[29] Although this is an important discussion, it is beyond the scope of this article to engage in a comparison with different conceptualisations of cyberspace in military doctrine. However, it is worth noting that US military doctrine sees cyberspace as a domain within the information environment. Joint Publication 3-12 (updated in 2022, but not publicly available), states: ". . . cyberspace, which is the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers." See *Joint Publication 3-12: Cyberspace Operations*, US Joint Chiefs of Staffs, June 8,

2.2 Cyberwarfare and Unpeace

As mentioned, cyberwar and cyberwarfare are often used interchangeably. As several scholars point out, however, it is essential to distinguish the two concepts from one another.[30]

In recent decades, much has been written on whether cyberwar would constitute a new form of conflict, fought by destructive virtual weapons rather than kinetic impact.[31] Without going into detail, at least two central problems with the concept pertain to intersecting conceptual, legal, and empirical issues.

First, talking about a cyberwar assumes, at least implicitly, that it could be an isolated war fought solemnly in cyberspace or in the cyber domain, understood as a domain of warfighting. This begs the question of where to draw the line in thinking about war. While discussing legal definitions of war with regard to national legislation and International Humanitarian Law (IHL), Yoram Dinstein states that "the term 'war' gives rise to more than a handful of definitional problems."[32] A conventional definition of the term is the following:

> War is a hostile interaction between two or more States, either in a material or in a purely technical sense. War in the purely technical sense is a formal status produced by a declaration of war. War in the material sense is generated by actual use of armed force, which is comprehensive on the part of at least one Belligerent Party.[33]

Following this definition, even if a cyberattack could initiate or escalate armed conflict, from the material perspective armed force would be a prerequisite for the threshold for war.[34] While it is a hypothetical possibility that a cyberattack could lead to massive destruction, equivalent to a kinetic armed force, for example by

---

2018, p I-1. In NATO doctrine, cyberspace is concepttualised in a similar manner, except that its relation to the information environment is less clearly stated. See *Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations*, Edition A Version 1, NATO, 2020, p 1–3.

[30] See, for example, Moore, *Offensive Cyber*.

[31] See Erik Gartzke, "The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no 2 (2013): 41–73; Adam P Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no 3 (2012): 401–28; Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no 1 (2012): 5–32.

[32] Yoram Dinstein, *War, Aggression, and Self-Defence* (Cambridge and New York: Cambridge University Press, 2017), p 17.

[33] The definition is from Dinstein, *War, Aggression*, p 17. It is however close to the Geneva Convention's statements on "war" and "armed conflict" definition in article 2.

[34] This is by no means the sole interpretation of the requirements for where to draw the line for the threshold of war. Dinstein represents a positivist stance on the matter whilst several other scholars, e.g. contextualists, have a more contextual view. See: Heather Harrison Dinnis, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), p 62, 74.

manipulating launching mechanisms for nuclear weapons, the impact of such an attack would not be restrained to the cyber domain.[35] Indeed, even if it meets the threshold for an act of war, the real-world impact will likely involve one or several other warfighting domains. As Moore argues: "[M]odern wars do not neatly constrain themselves to a single domain or set of capabilities."[36] So far, the destructive potential in malicious computer code does not reside in itself, but in its possibility to affect and manipulate targets outside of cyberspace.

Secondly, there needs to be more empirical evidence to support the claim that cyberattacks in themselves have ever lived up to the criteria of being acts of war, making the relevance of the concept of cyberwar even more questionable. In this vane, Kello argues: "If the effects of a cyberattack produce significant physical destruction or loss of life, the action can be labelled cyberwar, a term that should be used sparingly… given that no cyberattack to date meets this criterion." [37] Moore even suggests that cyberwar "simply [is] not a meaningful construct and may therefore be replaced with other more appropriate labels." [38] However, this does not mean that cyberattacks cannot be seen as a method of warfare within the context of war, either in the material or in the technical sense.[39]

Cyberwarfare is a more precise term than cyberwar. First, by talking about warfare and not war, cyberwarfare lends the benefit of avoiding the allusion that cyberspace is a free-standing domain of warfighting, or that a separate war could be waged in this domain. Nonetheless, appending "warfare" to "cyber" to form "cyberwarfare" is not an unproblematic endeavour. For example, within the context of war, Dinstein defines warfare as "the use of military force."[40] In armed conflict, cyberwarfare can thus be a relevant conceptualisation, since it is one of several warfighting measures that can be implemented to induce violence in concert with other measures. But, cyberwarfare is often used as an umbrella category for a broad range of cyber-related activities.

Thirdly, how do we understand hostile cyber activities that are not being conducted within the context of war? Denial of service, data manipulation, system manipulation, and espionage are typically identified in the literature as the main functions

---

[35] See Marika Ericson, *On the Virtual Borderline: Cyber Operations and their Impact on the Paradigms for Peace and War* (Uppsala: Uppsala University, 2020), p 257-260.

[36] Moore, *Offensive Cyber*, p 35.

[37] Kello, *The Virtual Weapon*, p 52.

[38] Moore, *Offensive Cyber*, p 17. Cf. Ericson, *On the Virtual*, p 173.

[39] Ericson, *On the Virtual*, p 173.

[40] Dinstein, *War, Aggression*, p 13. In UN Charter, "warfare" is used with restraint, and "force" was used instead of "war." See: Ericson, *On the Virtual*, p 213.

of hostile cyber activities.[41] If these activities are seen as cyberwarfare, then, confusingly and contradictorily, warfare is a term being applied to describe a context that may or may not be war. However, to quote Heather Harrison Dinnis, this does not imply that cyberattacks that do breach threshold of physical force are permissible: "It is likely that any computer network attack [cyberattack] severe enough to raise this question will be considered an unlawful interference in the affairs of a state, and may in all likelihood amount to a threat to the peace."[42]

Many scholars have argued that activities that aim to influence adversary conduct while operating below the threshold of technical and material warfare are conducted in the "grey zone,"[43] thus rendering the applicability of IHL and the right for an attacked state to self-defend unclear.[44] This term seeks to conceptualise hostile activities that occur between war and peace, which makes it particularly prevalent in discussions about cyberwarfare. Frank Hoffman describes grey zone conflicts as when "adversaries employ an integrated suite of national and subnational instruments of power in an ambiguous war to gain specified strategic objectives without crossing the threshold of overt conflict."[45] Instead of the grey zone, Kello suggests "unpeace" to conceptualise "the new range of rivalrous activity that falls between the binary notions of war and peace."[46]

While few scholars deny that there are both terminological and legal problems in conceptualising offensive borderline cyber activities, the term "grey zone" has been criticised for being ahistorical (namely, that it does not describe a new phenomenon per se) and that it is only one of many "terminological fads" (e.g., hybrid warfare, nonlinear warfare, and information warfare).[47]

---

[41] Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Hurst: London, 2022), p 15.

[42] Harrison Dinniss, *Cyber Warfare*, p. 74.

[43] For a critical discussion of the concept, see Tahir Mahmood Azad, Muhammad Waqas Haider, and Muhammad Sadiq, "Understanding Gray Zone Warfare from Multiple Perspectives," *World Affairs* 186, no 1 (2023): 81–104.

[44] For a deepened discussion of the cyberwarfare *jus ad bellum* (the right to wage war) and *jus in bellum* (the laws of war) in relation to cyberwarfare, see Harrison Dinniss, *Cyber Warfare*.

[45] Frank G Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," in *2016 Index of US Military Strength: Assessing America's Ability to Provide for the Common Defence*, ed Dakota L Wood (Washington: The Heritage Foundation, 2016), 25–36.

[46] Kello, *The Virtual Weapon*, p 17.

[47] Adam Elkus, "50 Shades of Gray: Why the Gay War Concepts Lacks Strategic Use," *War on the Rocks*, 15 December 2015: https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/.

Regardless of the degree of strategic effect that can be achieved through cyberspace,[48] even if state-led cyber operations typically "are not cyber-war but simply new types of age-old sabotage, espionage, and subversion," as Thomas Rid argues,[49] the escalating reach of cyberspace, the digitalisation of humanity and societies, and the increased connectivity of militaries have arguably brought about new cyber-enabled vulnerabilities and attack vectors. Since cyberspace is not bound to geographical constraints as the other domains are, the potential for sabotage, espionage, and subversion has increased, and a substantial number of offensive cyber activities are being conducted.[50] Moreover, many of these offensive activities are conducted by, or remaining in the good memory of, states with a more flexible understanding of the peace-war binary.[51]

Assuming that cyberspace indeed has changed the metrics of possibility between war and peace, the term *unpeace* is used in this report. Since unpeace is not war, cyberwarfare is understood, following Moore, as "a set of capabilities that act as a force multiplier in armed conflict" and that do "not supplant but rather complement existing military doctrine."[52]

For the topic of this report, this simple theoretical delineation means that cyberwarfare is a relevant term to use in discussing the Russo-Ukrainian war, which started in 2014. However, while Russia and Ukraine are not finding themselves in a situation of unpeace, NATO member states and many EU member states are arguably finding themselves in an explicit condition of unpeace vis-à-vis Russia.

---

[48] Kello exemplifies these outcomes with the manipulation of foreign governmental establishments, the destabilisation of economic and financial frameworks, the acquisition of military and fiscal resources, the incapacitation of public administrative and communicative structures, the impairment of civilian energy provisioning, and other analogous endeavours. Lukas Kello, *Striking Back: The End of Peace in Cyberspace – And How to Restore It* (New Heaven and London: Yale University Press, 2022), p 12.

[49] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no 1 (2012): 5-32.

[50] On cyberwarfare and conflict in relation to international relations and strategic outcome, see, for example, Richard J Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* 45, no 4 (2022): 534–67; Whyte and Mazanec, *Understanding Cyber-Warfare*, pp 137–142.

[51] For further discussion of the peace-war binary and its aptitude for countering hostile cyber activities, see Lucas Kello. "Cyber Legalism: Why It Fails and What to Do about It," *Journal of Cybersecurity* 7, no 1 (2021): 1–15. On China's and Russia's understanding of "cyber sovereignty" and how it differs from Western', see Harriet Moynihan, "The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace," *Journal of Cyber Policy* 6, no 3 (2021): 394–410, p 401–402.

[52] Moore, *Offensive Cyber*, p 6.

2.3 Campaigns, Operations, and Attacks

The terminology used in the field of "cyber" draws heavily on military terminology. Some of these terms are the already discussed cyberwar, cyberwarfare, and cyber domain; others are cyber campaigns, cyber operations, and cyberattacks. These terms name the hostile activities carried out in cyberspace. While military terminology may be relevant when discussing cyberwarfare, this may be to a lesser degree when discussing hostile cyber activities that are below the threshold of war. Moreover, as Richard J Harknett and Max Smeets highlight, there "is a tendency to treat terms such as 'breach,' 'cyberattack,' 'hack,' 'cyber incident,' and 'cyber operation' as synonymous, whilst in reality, they have different meanings and connotations."[53] In this report, cyber activities within the context of war and conflict are placed within the classical three-levelled framework: strategic (long-term planning and goals), operational (campaigns and operations), and tactical (cyber exploits and cyberattacks).

Following Harknett and Smeets, this report defines cyber campaigns as a consecutive series of orchestrated cyber operations unfolding over time. The overarching objective of cyber campaigns is attaining a cumulative outcome leading to strategic advantage.[54] In military terms, a strategic advantage refers to a favourable position or condition that enables one side in a conflict to achieve its goals and objectives more effectively than the opposing side. This advantage can manifest in various ways, such as superior positioning, intelligence, logistics, technology, or overall strategic planning. It allows the side with the advantage to exert greater control throughout the conflict and increases the likelihood of their achieving the desired outcomes.[55]

Cyber operation is a sub-category of cyber campaigns. It refers to "a series of coordinated actions directed towards a computer or network in order to achieve a certain operational objective."[56] Operational objectives may encompass a broad

[53] Harknett and Smeets, "Cyber Campaigns," p 541.

[54] Harknett and Smeets, "Cyber Campaigns," p 541.

[55] For a more qualified discussion of strategic advantage, see James Black, Diana Dascalu, Megan Hughes, and Ben Wilkinson, *Strategic Advantage: Definitions, Dynamics, and Implications*, RAND Europe, RAND Corporation, Santa Monica and London, 2023, p 40: https://www.rand.org/pubs/research_reports/RRA1959-1.html. On cyber capabilities as a tool for shaping the geopolitical environment to achieve strategic advantage, see Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge and London: Harvard University Press, 2020).

[56] Harknett and Smeets, "Cyber Campaigns," p 541.

spectrum of results, e.g., espionage, data destruction, system manipulation or destruction, and data theft.[57] These objectives are arguably quite different, and some have become standard procedures in interstate competition. Moore underscores that much that is characterised as cyberwarfare "is in fact routine intrusion operations conducted by intelligence agencies for broader peacetime national security objectives."[58] He thus suggests that a distinction be made between offensive military cyber operations within the context of war and conflict and other cyber activities carried out below the threshold of war.[59]

This leads to another important distinction. As Moore notes, not all cyber activities within the context of war and conflict are offensive cyber operations. He argues that "to lump all network intrusions as 'cyber' strips away crucial distinctions" by explaining that, for example, "grouping influence campaigns with destructive malware leaves much to be desired."[60] Concerning activities such as espionage, influence, and disinformation, it might thus be more precise to talk about cyber-enabled activities rather than cyber operations per se.[61] To put it bluntly, conducting an offensive cyber operation to hamper an army's command and control systems is quite distinct from hacking a user's account on Telegram to spread disinformation.[62] Thus, offensive military cyber operations concern "digitally affecting adversary systems and networks for a military goal or objective; affecting data by using data," which means that kinetic operations that attack the infrastructure of cyberspace are not seen as cyberwarfare.[63]

Moreover, within the framework of cyber campaigns, cyber operations can be directed toward various entities, typically involving military, government, finance, industry, and infrastructure computer networks and systems. They may be executed by various actors, commonly called Advanced Persistent Threat Actors (APT),[64] referring to states' official cyber actors, state-sponsored actors, state-supported actors, and other actors with advanced offensive cyber capability.

---

[57] Matthew Monte, *Network Attacks and Exploitation: A Framework* (Wiley: Indianapolis, 2015), p 4.

[58] Moore, *Offensive Cyber*, p 7.

[59] Moore, *Offensive Cyber*, p 7.

[60] Moore, *Offensive Cyber*, p 5.

[61] Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Bulletin of the Atomic Scientists* 75, no 4 (2019): 187–96.

[62] Moore, *Offensive Cyber*, p 37.

[63] Moore, *Offensive Cyber*, p 7.

[64] In the literature and in cyber security analysis, known APT actors are attributed a name and a number. However, while many analysts use the APT number, the name attributed to a group varies. For example, analysts use at least three names (i.e., Fancy Bear, Tsar Team, and Strontium) for APT28 (the group is commonly attributed to the Main Directorate of the General Staff of the Armed

Offensive cyber operations can be divided into event-based operations (immediate attacks against networks) and presence-based operations (lengthy intrusions that may culminate with an attack).[65] Both of these types of operations contain four consecutive phases: preparation (pre-planning), engagement (initial compromise of targeted networks and devices), presence (gradual infection and intelligence collection), and effect (direct or gradual impact).[66] Depending on the scope of the operation, the phases differ in the amount of resources and time needed.[67] The preparation and presence phase can last for years for high-impact operations.

In this conceptual understanding of offensive cyber activities, cyberattacks and cyber exploits are below operations (at the tactical level, in military terms).[68] The purpose of cyberattacks is to disrupt, deny, degrade, or destroy computer networks. One common form of cyberattack is distributed denial of service (DDoS) attacks, typically by flooding target networks with traffic, thus disturbing the target network, typically rendering websites inoperable. Other types are malware attacks that install code or software that tamper with the targeted networks. One prevalent form of malware that Russian APTs use is "wipers," which erase the target's data. It is essential to emphasise the extensive range of sophistication observed in offensive cyber activities. This spectrum spans from relatively basic DDoS attacks, which demand minimal technical skills, to highly advanced operations targeting critical infrastructure.[69]

Cyber exploits refer to the capability to take advantage of weaknesses in software applications, hardware components, network setups, and the human factor.[70] The purpose is mainly to conduct espionage and reconnaissance. The most common form of cyber exploits for breaching networks is so-called "phishing," which takes advantage of the human factor to lure users into giving away passwords or other sensitive information or lead to the installation of malware and spyware.

Forces of the Russian Federation, or GU). For further information, see Antoine Lemay, "Survey of Publicly Available Reports on Advanced Persistent Threat Actors," *Computers & Security* 72 (2018): 26–59.

[65] Moore, *Offensive Cyber*, p 76.

[66] Moore, *Offensive Cyber*, p 75. Compare with the kill-chain model from Lockhead Martin: Smeets, *No Shortcuts*, p 14.

[67] On resources and capabilities, see Smeets, *No Shortcuts*, p 73–92.

[68] This understanding draws on Monte's work on network attacks and exploits. This report uses the term cyber instead of network. See Monte, *Network Attack*, p 2.

[69] See Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford and New York: Oxford University Press, 2015), p 33-37.

[70] On network exploits, see Monte, *Network Attacks*, p 2. On the human factor, see Sambaluk, *Myths and Realities*, p 40–42.

As discussed, not all cyber operations lead to cyberattacks, since they can be cyber exploits. However, all cyberattacks are preceded by some form of cyber exploit. This is a crucial distinction when interpreting data on cyberattacks, since confusing exploits with attacks may significantly inflate the number of attacks.[71]

2.4 Conclusion

This chapter discusses central concepts in the research and analysis of cyber activities. Cyberspace is understood as encompassing all existing computer networks, connections, and means of control, extending beyond the internet to encompass diverse networks inaccessible from the public internet.

Whether cyberspace should be considered a distinct domain of warfare, the fifth domain alongside land, sea, air, and space, has elicited conceptual debates. Cyberspace's integration with other domains is increasing due to rapid technological advancements and connectivity. In this report, cyberspace pertains to the technical realm, while the cyber domain encompasses the human, social, and political aspects and is not a separate warfighting domain.

Distinguishing between cyberwar and cyberwarfare is imperative, despite their frequent interchangeability. The former term assumes, or at least tacitly implies, that conflict is isolated within the cyber domain, raising questions about the threshold for defining war. Supposing that war is taken to mean hostile interaction and the actual use of armed force, there are limitations in characterising malicious cyber activity, per se, as warfare, due to the prerequisite of physical force. Empirical evidence also fails to substantiate claims that known cyberattacks meet the criteria for acts of war. The term cyberwarfare hence offers a more precise description, considering its relevance within armed-conflict scenarios.

However, the term's applicability outside the context of war raises complexities, particularly concerning activities conducted below the threshold of war. Given cyberspace's evolving dynamics, this report refers to unpeace as the way to acknowledge the transformative possibilities between the metrics of war and peace. Offensive cyber operations, facilitated by increased connectivity and digitalisation, reveal new vulnerabilities and vectors, expanding the role of cyberspace in conflicts. Consequently, while cyberwarfare is relevant to the Russo-Ukrainian conflict, certain NATO and EU member states find themselves in a situation of unpeace in their interactions with Russia.

Although this report does not provide its own analysis nor classification of cyberattacks conducted during the Russo-Ukrainian war, these conceptual, definitional, and contextual issues remain important to bear in mind when interpreting reports of cyberwarfare. In this report, then, the term cyberwarfare is an umbrella category

[71] For further discussion on separating exploits from attacks, see Smeets, *No Schortcuts*, p 15.

that includes subcategories such as cyber campaigns, cyber operations, cyber exploits, and cyberattacks.

3 Russia's Hostile Cyber Activities in Ukraine

Russian APT actors have targeted Ukraine with a broad range of hostile cyber activities for over a decade. Since the end of 2013, several scholars and analysts have concluded that Ukraine has become a test lab for Russian cyber activities.[72] Many of these are described in the literature as case studies to develop cyber-warfare theory and to clarify what kinds of cyber activities and tactics Russia can use against Western countries.

Regarding hostile Russian cyber capabilities, the first thing to note is that there is no proper, official, cyberwarfare doctrine.[73] From a doctrinal perspective, Russian strategy is defensive, and is enshrined in several doctrines and policies from the early 2000s.[74]

While the official Russian standpoint is that they never interfere with the internal affairs of other states, it is likely, however, as Carolina Vendil Pallin explains, that there actually are policies or action plans for offensive cyber capabilities.[75] Several known Russian APT actors are directly under or tied to the military and civilian intelligence services, i.e., the Military Intelligence Service (GU), the Federal Security Service (FSB), and the Foreign Intelligence Service (SVR).[76]

---

[72] See, for example, Alina Polyakova, "Want to know what's next in Russian election interference?" *Brookings Institute*, 28 March 2019: https://www.brookings.edu/articles/want-to-know-whats-next-in-russian-election-interference-pay-attention-to-ukraines-elections/.

[73] A doctrine for civil cyber security was likely in the making in 2011, but was never turned into official doctrine, at least not publicly. For a thorough discussion on the issue in Swedish, see Carolina Vendil Pallin, *Nyckelaktörerna för rysk cyberstrategi: 2000–2020*, FOI-R--5025--SE, Totalförsvarets forskningsinstitut, Stockholm, 2020, p 31ff: https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5025--SE.

[74] For an in-depth discussion of the doctrines, policies, and development of cyber capabilities, see Andrei Soldatov and Irina Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities," CEPA, 2022: https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/. For a brief run-through of the doctrines and policies, see Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace* (Washington: Georgetown University Press, 2019), p 96–105.

[75] Vendil Pallin, *Nyckelaktörerna för rysk*, p 19: https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5025--SE.

[76] What follows is a short list of intelligence directorate and APT actors, and their respective target focuses. GU: APT28 (aka Unit 26165, Sofacy, Fancy Bear, and Tsar Team) focuses on data theft and phishing on military targets; Sandworm (aka Unit 74455, Vodoo Bear, and Electrum) focuses on data destruction and espionage; DEV-0856, is suspected to belong to GU, and focuses on destructive operations, data theft, and influence operations; CyberBerkut is likely Ukrainian but pro-Russian, with suspected ties to GU), and focuses DDoS attacks on Ukrainian state agencies. FSB: Gamaredon (aka Armageddon, Shuckworm, Primitive Bear, Winterflouder,

Conceptually, cyber capabilities are commonly seen within the framework of information confrontation.[77] From a Russian military theoretical point of view, this designates a permanent and confrontational state with the West, where Western states are seen as aggressors that seek dominance over their adversaries through information influence.[78]

This framework consists of two interrelated features; one is information-psychological, and the other is information-technological. From a generalised Western military theoretical standpoint, the former refers to cognitive aspects of information warfare and the latter to cyberwarfare capabilities.[79] This means that in the semi-official Russian perspective, what this report refers to as cyber operations are conceptually seen as tools for information influence. This conceptual focus on information is also apparent in how Russian leaders have approached what in the West is mostly seen as cyber security and cyber defence, i.e., information security.[80]

Against this background, this chapter presents and discusses known and suspected Russian cyber operations against Ukraine within this context. It begins with the premise that Russian cyber operations against Ukraine since 2014 are to be understood within the context of cyberwarfare.

BlueAlpha, BlueOtso, SectorC08, and IronTiden), focuses on phishing and data theft; Energetic Bear (aka Unit 71330) focuses on data theft; Summit (aka Turla Team, Snake, Uroburos, Venomous Bear, and UNC 4210), focuses on cyberespionage and phishing; InvisiMole (aka UAC-0035), focuses mainly on "spearphishing" against Ukrainian state agencies. SVR: APT 29 (aka. UNC2452/2652, Cozy Bear, and The Dukes), focuses on phishing against Western European governments and foreign policy groups). See Martti Lehto, "Cyber Warfare and War in Ukraine," *Journal of Information Warfare* 2, no 1 (2023): 61–75, p 61–65.

[77] Information confrontation (in Russian *информационное противостояние*) and information warfare, (in Russian *информационная война*) are sometimes used interchangeably in Russian military and academic texts. Michelle Grisé et al however showcase that information confrontation is likely best understood as an umbrella category out of which information warfare is one distinct feature. See Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W Welburn, and Khrystyna Holynska, "*Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation*," RAND Corporation, Washington, 18 August 2022: https://www.rand.org/pubs/research_reports/RRA198-8.html.

[78] Grisé et al, *Rivalry in the Information*, p 98.

[79] Grisé et al, *Rivalry in the Information*, p 11.

[80] On Russian information security and control of information in Russia, see Jaclyn A Kerr, "Runet's Critical Juncture: The Ukraine War and the Battle for the Soul of the Web," *SAIS Review of International Affairs* 42, no 2 (2022): 63–84; Carolina Vendil Pallin, *Moscow´s Digital Offensive: Building Sovereignty in Cyberspace*, FOI Memo 7521, Swedish Defence Research Agency, Stockholm, 2021: https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI%20Memo%207521.

3.1 Ukraine as a Test Lab

Ukraine was far from the first country targeted by Russian cyber operations and cyber-enabled information influence. In 2007, Russian actors used a politically sensitive issue to enflame tensions between pro-Russian Estonians and the reformist Prime Minister, Andrius Ansip. Large-scale cyber operations consisting of DDoS attacks were launched, targeting government websites, media organisations, and banking services, temporarily disturbing communications and the functionality of targeted websites. These cyber operations were coupled with an information influence campaign and the application of political pressure from Russia. Among other events, the lower house of the Russian parliament (the Duma) declared that the Estonian government glorified Nazism.[81]

This was the first major event where Russia showed its card regarding its offensive take on information confrontation. It was followed by cyberwarfare operations, in tandem with kinetic warfare, in Georgia (2008) and Syria (2015–),[82] as well as many cyberoperations, coupled with cyber-enabled information influence campaigns, in Bulgaria, France, Germany, Montenegro, Norway, and the US.[83]

The first known major hostile Russian cyber activities occurred in Ukraine in December 2013 (see Figure 1 for an overview of the discussed activities). They were conducted amid the protests against President Victor Yanukovich (a.k.a. Euromaidan), at the Independence Square (*Maidan Nezalezhnosti*) in central Kyiv, which later developed into the Revolution of Dignity. When it became clear that the protesters were not intending to leave central Kyiv, cyberattacks against the president's opposition started. Initially, the attacks consisted of DDoS attacks run from commercial botnets, but developed in sophistication when the violence escalated. In an attempt to cut the opposition's communications, cell phones were flooded with text messages and calls.[84]

In the run-up to Russia's illegal annexation of Crimea, in February 2014, which in hindsight can be seen as the start of the invasion of Ukraine, Russian and pro-Russian actors used various methods to gain informational control of the penin-

[81] For a complete account, see Bilyana Lilly, *Russian Information Warfare: Assault on Democracies in the Cyber Wild West* (Annapolis: Naval Institute Press, 2022), p 44–55.

[82] On Georgia, see David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* (2011): 1–10: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf. On Syria, see Austen Givens, "Putin's Cyber Strategy in Syria: Are Electronic Attacks Next?" *Cyber Defense Review*, 17 November 2015: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136170/putins-cyber-strategy-in-syria-are-electronic-attacks-next/.

[83] On cyber-enabled influence campaigns, see Lilly, *Russian information*.

[84] See Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington: Georgetown University Press, 2022), p 55–56.

sula. Ukrtelecom, the Ukrainian telecommunications operator, experienced incursions at its regional facilities, resulting in the severance of phone and internet connectivity. Media entities encountered physical obstructions preventing access to the peninsula. Additionally, elected representatives in the local parliament encountered impediments in their telecommunication services, coupled with the presence of troops (aka "the little green men"). On 16 March, a staged referendum showed that 93% of Crimeans favoured the annexation.[85] It is also worth noting that during this period, the Kremlin, who had early understood the importance of television for the purpose of information influence, tightened its control of social media platforms popular both in Russia and Ukraine.[86]

At the same time, pro-Russian and anti-Revolution of Dignity activities took place in the Eastern Donbas Region. Separatist and Russian proxy militias, the People's Militia of the Donetsk People's Republic and People's Militia of the Luhansk People's Republic, seized governmental structures. Shortly thereafter, they declared the oblasts of Donetsk and Luhansk as independent republics. Under the banner of an anti-terrorist operation, Ukraine managed to fight back the separatist insurrection in some areas, but when regular Russian troops rolled into Ukraine in late August, the war turned into a new phase.[87] During the initial phase of the war, Russian actors sought to isolate the regions, in terms of information. Cyber operations (see Chapter 2) were increasingly used against military communications to disrupt them and target soldiers via their personal cell phones. Cyber-enabled psychological operations were directed at Ukrainian soldiers. For example, demoralising text messages were sent to soldiers and their families. The cyber operations were facilitated by the fact that many Ukrainians were using Russian digital platforms for their communications.[88]

During the presidential election in May of the same year, 2014, the Ukrainian Central Election Commission suffered DDoS attacks, resulting in delays in reporting the results. Meanwhile, a fabricated election result started circulating; it claimed Dmitry Yarosh, from the Ukrainian Right Sector party, as the winner.[89] In Russian news reporting, the party was depicted as neo-Nazi, feeding the influence campaign of depicting Ukraine as a hotbed for neo-Nazism. The party won two regional seats in the parliamentary election in October of the same year.

---

[85] See Jasper, *Russian Cyber*, p 56.

[86] On the Kremlin, Telegram, and VKontakte, see: Nickolay Kononov, "The Kremlin's Social Media Takeover," *The New York Times*, 10 March, 2014: https://www.nytimes.com/2014/03/11/opinion/the-kremlins-social-media-takeover.html.

[87] Serhii Plokhy, *The Russo-Ukrainian War* (Dublin: Allen Lane, 2023), p 126-131.

[88] See Jasper, *Russian Cyber*, p 58.

[89] See Jasper, *Russian Cyber*, p 58.

In 2015–2017, Russian APT actors displayed increased capabilities in destructive cyber operations. In 2015, an operation was launched against the power grid in Kyiv. Employing a combination of spearphishing e-mails and malware, the attackers took remote control of local power stations outside the city and deployed wiper malware. This led to a widespread power outage, impacting approximately 230,000 customers. The operation also included denial of service attacks against the call centres of the power company, thus leaving customers in the dark.

Although it was a sophisticated operation, with many synchronised attacks, which also demanded extensive reconnaissance, the power outages only lasted for one to six hours.[90]

In 2016, another sophisticated operation was launched against the power grid in the capital. The attackers used malware that targeted networks and equipment, including protective relays.

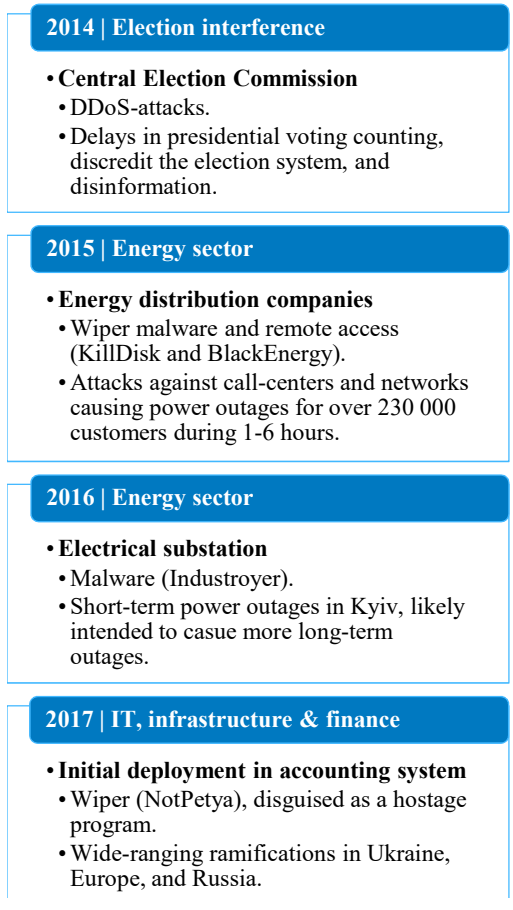

Figure 1 – Russian campaigns and operations, 2014–2017

These relays had a weakness that made them need a manual restart after receiving a certain type of message. Even though the supplier, Siemens, had released a patch for this defect in 2015, many of these relays had not been updated. The operation followed a carefully planned series of steps, the first of which was to cause a widespread power outage by turning off all the circuit-breakers.

[90] Anton Cherepanov, *WIN32/Industroyer: A New Threat for Industrial Control Systems*, ESET, 2017: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf.

Then, an hour later, the attackers used another type of harmful software to disable the station's computers, making it impossible to monitor the progress of events. They also tried to disable certain protective relays, which wouldn't have been noticed by the operators. The attackers wanted the operators to turn the equipment back on, which would have initiated a large-scale attack and severe power outages, likely lasting for months. Due to some operational mistakes and possibly because the operators responded faster than expected, the attackers' plan didn't proceed as likely planned.[91]

In 2017, the NotPetya operation was launched, which to date is the most destructive known cyber operation. NotPetya is the name of a malware, which, disguised as ransomware, was a worm for the purpose of data-destruction. Through extensive reconnaissance and preparations, the malware exploited a vulnerability in Ukrainian accounting software and spread quickly throughout Ukrainian networks. It targeted critical systems, affecting government agencies, banks, and energy companies. However, the malware was not contained in Ukraine, thus affecting businesses and organisations worldwide, even in Russia. NotPetya caused extensive damage, rendering systems inoperable and leading to significant financial losses, estimated at USD 10 billion.[92]

Russia's cyber activities during its first invasion of Ukraine showcase how cyber operations were integrated into information influence campaigns to gain informational superiority and control, i.e., cyber-enabled information warfare. Moreover, these campaigns illustrate Russia's unconventional warfare strategy to occupy territory without relying on conventional and overt military capabilities and use the toolbox of information confrontation to influence politics and society in the targeted country and abroad.[93]

However, none of the cyber operations were of a scale that could disrupt Ukraine in their own right. From the Russian perspective, the successful annexation of Crimea and the fracturing of the Donbas region were likely more the result of Ukraine's being caught off guard, combined with indifference from the international community, than a demonstration of cyberwar.

---

[91] Cherepanov, *WIN32/Industroyer*.

[92] Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now," CSO, 17 October 2017: https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-not petya-malware-what-you-need-to-know-now.html.

[93] On the much debated Russian "hybrid" or "grey-zone" warfare, see: Christopher S Chivvis, *Understanding Russian "Hybrid Warfare" and What Can be Done About It*, RAND, Santa Monica, 2017, p 2–3:
https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf; James C Pearce, "Hybrid" and "Information": New Labels, Old Politics," in *Hybrid Conflicts and Information Warfare: New Labels, Old Politics*, eds Ofer Fridman, Vitaly Kabernik, and James C Pearce (Lynne Rienner Publishers: Boulder and London, 2019), 1–8.

3.2 From Test Lab to Full-scale War

Months before the full-scale invasion, there was a significant increase in hostile Russian cyber activities. These included event- and presence-based operations and numerous cyber-enabled information operations against military and civilian targets. According to Illia Vitiuk, Head of the Department of Cyber and Information Security of the Security Service of Ukraine (SBU), Ukraine was targeted by 4200 cyberattacks in 2022, compared to 1400 in 2021.[94] The cyber-security company, Mandiant, describes a higher frequency of severe cyberattacks in Ukraine within the initial four months of 2022 compared to the preceding eight years.[95]

Google, which has been supporting Ukraine with analysis, security, and defence in cyberspace, divides the run-up to the invasion and the first year of hostile Russian cyber activities into five phases.[96] During the first phase (2018 to January 2022), Russian threat actors conducted cyberespionage and pre-positioning in Ukrainian networks. The second phase (February to April 2022) coincided with the initial phase of the full-scale invasion and was signified by destructive cyber operations and cyber-enabled information operations. The State Service of Special Communications and Information Protection of Ukraine concludes that during the planning and active phases of the invasion, cyberespionage, destructive actions, and influence operations were closely linked to facilitate more effective on-the-ground operations.[97] This involved identifying covert Ukrainian defenders in occupied territories and eliminating potential partisans. This fits the pattern of Russia's irregular warfare strategy,[98] i.e., cyber operations were mainly executed in tandem with influence operations to shape the information environment and to support the Russian narrative of a "special operation", intended to return the Ukrainians to their true historical Russian path.[99]

---

[94] Vitiuk interviewed in: Alperovich and Gray, "How Russian."

[95] Google, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*, Mountain View: Google Inc, 2023, p 13: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

[96] Google, *Fog of War*, p 15.

[97] *Russia's Cyber Tactics: Lessons Learned 2022*, State Service of Special Communications and Information Protection of Ukraine, Kyiv, 2023: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine.

[98] Damjan Štrucl, "Russian Agression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare," *Contemporary Military Challenges* 24, no. 2 (2022): 103–123, p 2–3.

[99] For an indepth discussion on the Russian motives for the full-scale invasion, see Carolina Vendil Pallin, Maria Engqvist and Carl Michael Gräns, "Russia's national security: fighting the West for regional hegemony," in *Russia's War Against Ukraine and the West: The First Year*, eds Maria Engqvist and Emil Wannheden, FOI-R--5479--SE, Swedish Defence Research Agency, Stockholm,

The third phase (May to July 2022) saw sustained targeting and attacks followed by the fourth phase (August to September 2022), which was sustained presence to gain strategic advantage. In the fifth phase (October to December 2022), Russian actors launched a new campaign of disruptive attacks. Other accounts emphasise that the sophistication of the attacks decreased in the month following the full-scale invasion, with an increasing focus on DDoS attacks and simpler exploits targeting everything from government websites to local businesses.[100] Several sources indicate that, during 2023, hostile Russian cyber activities, such as cyber-

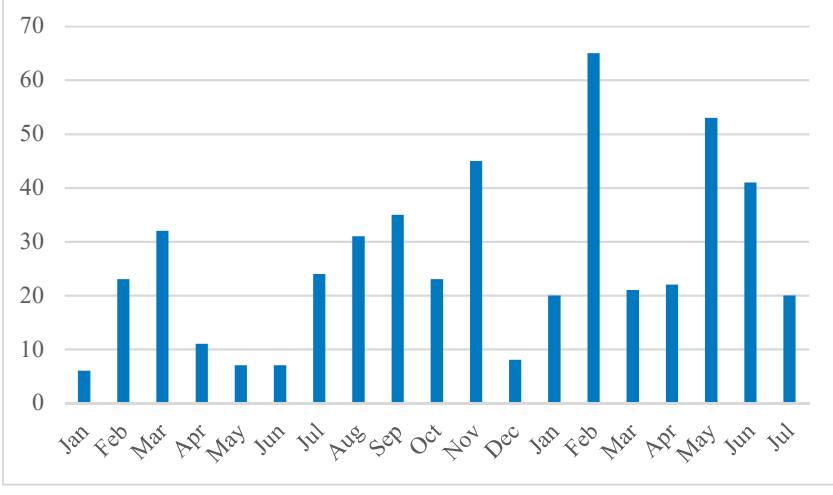

Figure 2 – Cyber operations against civilian targets. Cyber Peace Institute, as of 12 September 2023.

exploits within military networks used to locate Ukrainian troops and nodes of communication, have been becoming more sophisticated.[101] This would mark a shift in the usage of cyber capabilities on the battlefield since earlier assessments indicate that the geolocation of Ukrainian troops has mainly been carried out with UAV reconnaissance, electronic warfare, acoustic reconnaissance, and radar.[102]

2023, 33–44: https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5479--SE.

[100] See Vitiuk, interviewed in Alperovich and Gray, "How Russian."

[101] See, for example, Daryna Antoniuk, "Russia's Turla Hackers Target Ukraine's Defense with Spyware," *The Record: Recorded Future News*, 19 July 2023: https://therecord.media/turla-hackers-targeting-ukraine-defense.

[102] Bateman, "Russia's Wartime," p 26.

At the time of writing, the Cyber Peace Institute has mapped 494 cyberattacks and operations (Figure 2) against civilian targets.[103] Of these, 374 have been disruptive DDoS attacks, 30 have been malware, 17 have been defacement, and 17 have been wipers, followed by espionage and other exploits the institute includes in its data.[104]

Regarding targets (Figure 3), public administration has been the most affected sector, followed by infrastructure (information and communication technology, or ICT; transportation; energy; and water); the financial sector; news media and, to a lesser degree, the education, manufacturing, health, and agriculture sectors.

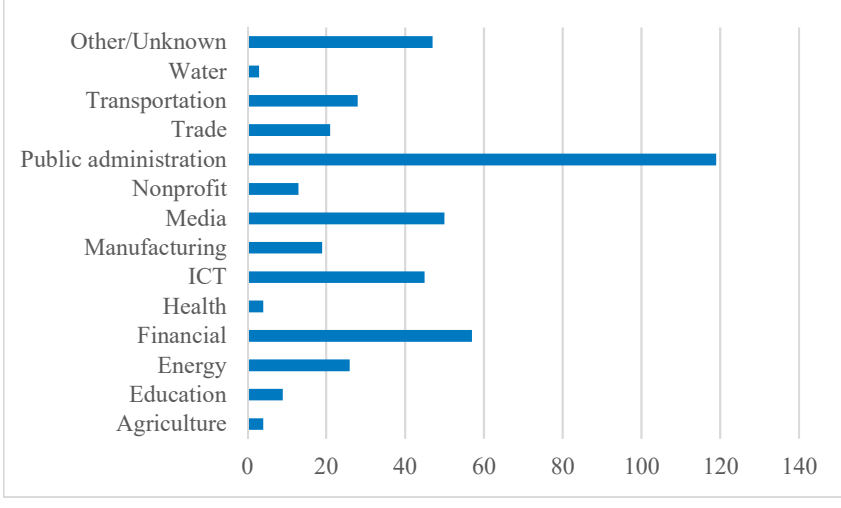

Figure 3 – Civilian targets. Cyber Peace Institute, as of 12 September 2023.

It is more challenging to assess hostile activities against military targets, due to a lack of aggregated data. Ukrainian sources show that Russian cyber campaigns have been launched against military web resources, information about military

[103] Cyber Peace Institute, Impact, accessed 17 September 2023: https://cyberconflicts.cyberpeaceinstitute.org/impact.

[104] The Cyber Peace Institute includes surveillance and cyber-enabled information operations in this data; therefore further in-depth analysis is needed to assess the data from the perspective of this report's conceptual understanding of hostile cyber activities. The Cyber Peace Institute defines a cyberattack and operation as an "incident conducted by a threat actor using a computer network or system with the intention to disrupt, disable, destroy, control, manipulate, surveil or extract a computing environment/infrastructure and/or data." See Cyber Peace Institute, Data and Methodology, accessed 17 September 2023: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology.

personnel and veterans, military recruitment centres, the Security Service of Ukraine, and the defence industry.[105]

There are a few publicly available documented cases when Russian cyber operations correlate with kinetic operations. For example, in the northeastern Ukrainian city of Sumy, suspected Russian APT actors were present in local networks from 17 February, 2022. On 24 February, Russian tanks moved towards the city; on 3 March, there were widespread electrical power outages, including kinetic attacks against the power grid. Another case concerns the Russian occupation of the Zaporizhzhia nuclear power plant, on 3 March. The preceding day, Russian APT actors were present in Energoatom's networks, although it is unclear what this presence implied.[106] In yet another example, on 11 March, a government agency in Dnipro, in eastern Ukraine, was targeted by destructive cyberattacks, followed by missile strikes against government buildings.[107]

Regarding Russian APT actors, groups within and tied to the intelligence services have been at the forefront regarding presence-based and sophisticated cyber operations and cyber-enabled information-influence operations. Based on data from the Cyber Peace Institute, the APT actors that stand out are Sandworm (GU); FancyBear (GU); Cadet Blizzard (GU); the Belarusian APT group, UNC1151; Summit; and Gamaredon. However, the most active groups are hacker collectives,[108] especially if cyber operations against other European and North American countries are included.[109] The most prominent groups among them are NoName057(16), People's

---

[105] Volodymyr Shypovskyi, "Cyber Domain in Russian-Ukrainian War 2022," presentation, *Defending Ukraine: The Changing Face of Cyberwarfare*, Swedish Defence University, Stockholm, 23 August 2023.

[106] Shypovskyi, "Cyber Domain."

[107] *Defending Ukraine: Early Lessons from the Cyber War*, Microsoft, 2022, p 8: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

[108] The degree of independence from the Russian state is questionable. Illia Vitiuk, the head of the Cyber Security Department of the Security Services of Ukraine (SBU), for example, is reported to have stated that "There is no Russian hack [collective], actually; well, maybe it's a small, small percentage, but in fact, all of these groups like Killnet, Anonymous and Cyber Army of Russia with Deep Rock, etc, etc, we do believe that these are all groups created or orchestrated by the [Russian intelligence agency] GRU." In: Diego Laje, "Ukraine's Fusion of Cyber and Kinetic Warfare: Illia Vitiuk's Stand Against Russian Cyber Operations," *Signal (AFCEA International)*, 15 September 2023: https://www.afcea.org/signal-media/test-signal-landing-page-format/ukraines-fusion-cyber-and-kinetic-warfare-illia.

[109] See Google, *Fog of War*, p 12; Tom Hegel and Aleksandar Milenkoski, "NoName057(16) – The Pro-Russian Hacktivist Group Targeting NATO," *SentinelLabs*, 12 January 2023: https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/; *Anonymous Sudan: Threat Intelligence Report*, Truesec, Stockholm, 2023: https://www.truesec.com/hub/report/anonymous-sudan-threat-intelligence-report; Waqas, "List of Proxy IPs Exposed to Block Killnet's DDoS Bots," *HackRead*, 8 February 2023: https://www.hackread.com/killnets-proxy-ips-blocks-ddos-bots/.

Cyber Army, Anonymous Russia, and Killnet. Most of these groups' cyber operations are DDoS attacks and cyber-enabled information operations. It can even be argued that the main effect of some of these collectives is informational, having the purpose of creating "fear and uncertainty," as the cyber security company, Truesec, suggests.[110] For instance, cyberattacks have been carried out in relation to political proceedings unfavourable to Russia.

In November 2022, the website of the EU Parliament suffered from a DDoS attack in connection to the vote to declare Russia a state sponsor of terrorism.[111]

Sweden's NATO-accession process has also been a pretext for DDoS attacks against organisations and critical infrastructure.[112]

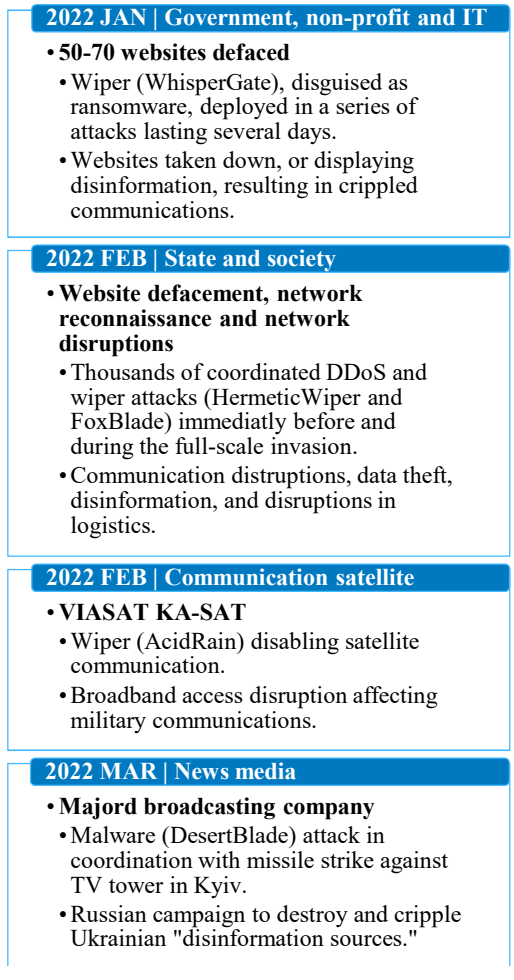

Figure 4 - Russian campaigns and operations, 2022-2023

Moreover, many of the groups are quite active on social media, where they gather substantial groups of followers. Killnet's Telegram channel has over 90,000 followers. They often catch the attention of national and international news media with headline-

[110] "'Anonymous Sudan': Most Likely Russia Attempting to Disrupt Sweden's NATO Application," Truesec, 20 February 2023: https://www.truesec.com/news/anonymous-sudan-most-likely-russia-disrupting-swedens-nato-application.

[111] Shannon van Sant and Clothilde Goujard, "European Parliament Website Hit by Cyberattack after Russian Terrorism Vote," *Politico*, 23 November 2022: https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/.

[112] "Anonymous Sudan," Truesec.

friendly names and bold statements.[113] For example, in September 2023, what are likely a dozen pro-Russian hacker groups published a video on social media that declared their joint effort to "de-nazify" Estonia, Latvia, Lithuania, and Poland.[114]

Google highlights that the cyber-criminal ecosystem has been reconfigured since the full-scale invasion, partly due to the divergence of political allegiances. For many of the groups, an earlier taboo against attacking Russia also appears to have weakened.[115] John Hultquist, vice president of intelligence analysis at Mandiant, is reported to have stated that another development is the commodification of the cyber-threat landscape, coupled with increased interaction between states and capabilities in the cyber-criminal ecosystem.[116]

At the time of writing, the impact of hostile Russian cyber activities during 2022 and 2023 is being debated amongst analysts and scholars (see next chapter for an in-depth discussion). By looking more closely at the more intense phase of sophisticated presence-based campaigns and operations that occurred during the initial phase of the full-scale invasion, it is possible to appreciate the scale and impact of Russian cyberwarfare (Figure 4).[117]

On January 13, a large-scale cyber operation targeted multiple organisations in Ukraine. The malware, named WhisperGate, masquerades as ransomware, but lacks a ransom recovery option, indicating that its destructive intent is to render targeted devices inoperable rather than seeking a ransom. The victims include various government, non-profit, and IT organisations. A Ukrainian IT firm also confirmed discovering the WhisperGate malware on some of its systems. Notably, out of the 70 sites marked for defacement, around 50 were developed and managed by this same Ukrainian IT firm. The compromising of this company allowed the hack-

---

[113] The argument that these groups are to a large degree part of information-influence campaigns can be strengthened by the fact that their pre-announcements of attacking a certain organisation and country
are counterproductive, since the threats likely make the targets of the announcements more aware of their impending activities. It is almost as if a house burglar were to call the house owner to announce the date of the robbery. However, it can also be argued that announcements prior to the fact are part of the cyber exploit itself, given that these groups are already surveilling potential targets and can thereby identity not only what measures the targets take but what they deem to be functions that are especially worthy of protection.

[114] Accessed on X, 6 September 2023.

[115] Google, *Fog of War*, p 41.

[116] Jenna McLaughlin, "Russia Bombards Ukraine with Cyberattacks, but the Impact Appears Limited," *NPR*, 3 March 2023: https://www.npr.org/2023/02/23/1159039051/russia-bombards-ukraine-with-cyberattacks-but-the-impact-appears-limited. See, also, Google, *Fog of War*, p 44.

[117] This summary is based on Cyber Peace Institute's timeline analysis: Cyber Peace Institute, Ukraine Platform, accessed September 17, 2023:
https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

ers to access its administrator panel and utilise its credentials to deface its customers' websites. On 14 January 2022, the Orthodox New Year, over 70 Ukrainian government websites were defaced with political imagery and messages in Russian, Ukrainian, and Polish, temporarily disrupting their services; part of one of the messages posted on the websites read "prepare for the worst."

The attack severely impacted the government's digital infrastructure, particularly the primary platform for online government services, which also plays a crucial role in Ukraine's COVID-19 response and vaccination efforts. The sites of several ministries, including those related to energy, sports, agriculture, veterans' affairs, and ecology, were also affected.[118]

An extensive cyber campaign was launched during the weeks leading up to the full-scale invasion. The campaign started on 15 February and peaked on the 23rd. During the campaign, Ukraine experienced its largest DDoS attack to date, causing several Ukrainian websites to go offline and affecting banks, government, and military websites. Approximately ten key Ukrainian websites, including the Defence Ministry, Foreign Ministry, and major state banks, became inaccessible during these attacks. Bank customers reported issues with online payments and banking apps, with some encountering difficulties accessing ATMs. Simultaneously, fraudulent SMS messages were sent to Ukrainian phones to incite panic. Moreover, more than 600 websites belonging to the Ministry of Defence and other institutions in Kyiv were targeted in attacks using thousands of exploits aimed at 20 distinct vulnerabilities, at least. The aim was likely to breach various targets, including the Border Defence Forces, the National Bank, and railway infrastructure, with the intent to steal data and disrupt essential defence and civilian infrastructure. Numerous systems across government, information technology, finance, and energy sectors were impacted, with notable intrusions affecting the State Nuclear Regulatory Inspectorate and the Ukrainian Investigation Website focused on Hazardous Waste. Additionally, several Ukrainian banks and government departments, such as the Ministries of Foreign Affairs, Defence, Internal Affairs, the Security Service (SBU), and the Cabinet of Ministers, faced DDoS attacks that resulted in temporary website inaccessibility, with some issues lingering into the following day.[119]

---

[118] For more details, see Christoffer Strömblad, "State-Sponsored Cyber Attacks Against Ukraine," *Trusec*, 19 January 2022: https://www.truesec.com/hub/blog/state-sponsored-cyber-attacks-against-ukraine.

[119] For more details, see "Update: Destructive Malware Targeting Organizations in Ukraine," Cybersecurity & Infrastructure Agency, United States Government, 28 April 2022: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a; Juan Andres Guerrero-Saade, "HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine," *SentinelLabs*, 28 February 2022: https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/.

On the first day of the full-scale invasion, a cyber operation targeted Viasat's KA-SAT broadband satellite, disrupting the company's internet services. This operation targeted the modems responsible for communicating with the satellite and providing internet access to customers across Europe, including Ukraine. The impact was significant, with some users experiencing more than two weeks of internet downtime. The incident affected tens of thousands of customers in Ukraine and throughout Europe. In France, nearly 9000 subscribers of a satellite internet service were affected, and about one-third of the 40,000 subscribers of another European satellite internet provider (covering Germany, France, Hungary, Greece, Italy, and Poland) experienced disruptions. A prominent German energy company also lost its remote monitoring access to more than 5800 wind turbines. Analysts found that a new wiper malware, named "AcidRain," was used in the operation.[120]

On March 1, a Russian APT actor deployed the so-called "DesertBlade" malware against a prominent broadcasting company. This incident coincided with the Russian military's announcement of its plan to target "disinformation" sources in Ukraine, leading to a missile strike on a TV tower in Kyiv.[121] At the time, it was reported that the consequence of this attack was a disruption of the Ukrainian public's access to a critical information outlet.[122]

3.3 Conclusion

Russia's offensive cyber activities during 2014–2022 were sophisticated, but none were cataclysmic. Lennart Maschmeyer and Myriam Dunn Cavelty argue that the recorded activities, those involving Crimea excepted, had negligible strategic value, although they do highlight the fact that the NotPetya operation significantly impacted Ukraine's GDP.[123] However, the strategic value is questionable, given

[120] For more details on the operation, see Juan Andres Guerrero-Saade and Max van Amerongen, "AcidRain | A Modem Wiper Rains Down on Europe," *SentinelLabs*, 31 March 2022: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

[121] Digital Security Unit, *Special Report: Ukraine - An Overview of Russia's Cyberattack Activity in Ukraine*, Microsoft, 2022, p 12: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[122] "Russians Struck at Kyiv TV Tower," Ukraine Institute of Mass Information, 1 March 2023: https://imi.org.ua/en/news/russians-struck-at-kyiv-tv-tower-i44122.

[123] The authors do not define strategic value, wherefore it is difficult to evaluate their analysis further. See Lennart Maschmeyer and Myriam Dunn Cavelty, "Goodbye Cyberwar: Ukraine as Reality Check," *Policy Perspectives* 10, no 3, CSS ETH Zürich, 2023, p 2: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf.

that the malware also reached Russia and led to sanctions against it.[124] The operation also revealed the intricate complexity of controlling potent cyber operations.

The cyber-enabled information campaign leading to the illegal annexation of Crimea arguably bore strategic value. Based on this period, the impact of offensive cyber operations relies upon their potential to be part of an irregular warfare campaign that focuses on informational control and provoking distrust amongst the population. Marcus Willet even suggests that "perhaps the most noteworthy aspect of Russia's two wartime uses of offensive cyber before the 2022 conflict was their limited nature. They mostly equated to low-level cyber vandalism, with the blocking of Georgian Internet access coming closest to being a major disruption."[125]

Moving into the period of the full-scale invasion, few of the recorded cyber operations, if any, bear resemblance to having kinetic impact, even if the Russian intention in many cases arguably were to have this kind of impact. As discussed in more detail in the following chapter, the cyber operation against the Viasat communications satellite is the closest to a resemblance of kinetic impact. The potential of cyber operations to deliver significant strategic value through multidomain operations is questionable, at least given the data available for this report. Although there are many recorded instances of cyber operations preceding kinetic attacks, a correlation between cyber and kinetic operations does not necessarily mean causation. However, it is underscored that the massive number of campaigns and operations conducted in 2022 and 2023 are to be considered far more than "cyber vandalism." Moreover, the reported increase of Russian APT actors in gaining access to Ukrainian military networks and soldiers' digital devices perhaps shows the most potent wartime usage of cyber operations, i.e. as a force multiplier to shape the battlefield.

[124] The authors do not define strategic value, wherefore it is difficult to evaluate their analysis further. See Lennart Maschmeyer and Myriam Dunn Cavelty, "Goodbye Cyberwar: Ukraine as Reality Check," *Policy Perspectives* 10, no 3, CSS ETH Zürich, 2023, p 2: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf.

[125] Marcus Willett, "The Cyber Dimension of the Russia–Ukraine War," *Survival* 64, no 5 (2022): 7–26, p 11.

4 What Happened to the Cyberwar?

Even when the supposedly second-most-capable warfighting power in the world, with a renowned capability in cyberwarfare, was launching its full-scale invasion of Ukraine, the role of offensive cyber campaigns and operations appeared to fail to live up to the expectations of many. Many experts argue that, at best, cyber operations are force-enablers in multidomain kinetic operations and influence operations, but they are hardly a potent weapon in their own right. As Marcus Willet argues, it was evident at the beginning of the war that Russia did not possess the cyber capabilities required to incapacitate Ukrainian weapon systems and military units precisely. Consequently, the Russians became dependent on conventional kinetic military means.[126]

If these general observations about the effect of Russia's offensive cyber operations during the Russo-Ukrainian war are correct, their conclusions are likely premature. Without more comprehensive data, especially regarding cyber operations against military targets, there are too many uncertainties involved in delivering a final verdict on the role of cyber operations in this war. For this reason, the primary purpose of this report is to discuss the prevalent hypotheses for explaining the lack of a large-scale "cyberwar."

This chapter discusses four hypotheses: wrong expectations, failed capabilities, failed analysis, and successful defence. The final hypothesis, a failed understanding of cyberwarfare, forms the basis for the concluding discussion in the following chapter. As mentioned (in Chapter 1), the hypotheses presented here consist of thematically ordered arguments from published articles and reports on cyberwarfare in the Russo-Ukrainian war.

4.1 Wrong Expectations

The first hypothesis about the lack of a large-scale cyberwar suggests that we are not seeing strategic effects from Russian cyberwarfare because the expectations about Russian capabilities were wrong. Undoubtedly, far from every analyst and scholar of cyberwarfare expected the Russians' code to cause significant destruction in Ukraine. However, since several distinguished experts did express these expectations, this hypothesis is no simple straw man.

As discussed above, Keir Giles stated that a "destructive cyber onslaught" potentially "could target military command and control systems or civilian critical infrastructure and pressure Kyiv into concessions and its friends abroad into meeting

[126] Willet, *The Cyber Dimension*, p 14.

Russia's demands."[127] A senior official of the Biden Administration stated that "Russia could opt to launch a sweeping cyber and disinformation campaign against Ukraine and its government rather than a traditional military invasion of the country."[128] William Courtney and Peter A Wilson suggested that Russian cyber operations could lead to "'shock and awe,' causing the collapse of Ukraine's defences or will to fight to collapse."[129] In early 2022, John Healey, renowned scholar on the history of conflict in cyberspace, wrote that the fact that a worst-case-scenario-attack has not yet happened, "may have less to do with the cyber capabilities themselves than with the behaviour of states during the relatively peaceful decades since the end of the Cold War."[130] Barely a month before the full-scale invasion, the journalist and cyberwarfare expert, Maggie Miller, pondered whether the "potential Russian invasion of Ukraine could give the world its first experience of a true cyberwar."[131] While the attacks in January, she wrote, "raised concerns, they were only a hint of Russian cyber capabilities," which "could take down the power grid, turn the heat off in the middle of winter and shut down Ukraine's military command centres and cellular communications systems."[132]

These expectations should be read against the background of hostile Russian cyber activities in the last decades. Russian cyber and influence operations in Estonia, Georgia, Crimea, Syria, the US and, not least, Ukraine, have been elevated by some into a mythical image of Russia as a mighty cyber power possessing an uncanny capability to control and manipulate the populations of other nations through the shadows.[133] The Kremlin has mirrored this image. For example, in 2016, Putin alluded that we were in the same situation now as when the atomic bomb made the US take the Soviet Union seriously: "I'm warning you: we are on the verge of having 'something' in the information area, which will allow us to talk to Americans as equals."[134] This type of posturing, supported by a Western myth of Russia

---

[127] Keir Giles, "Putin Does."

[128] Matishak, "Russia Could."

[129] Courtney and Wilson, "If Russia."

[130] John Healey, "Preparing for Inevitable Cyber Surprise," *War on the Rocks*, January 12, 2022: https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/.

[131] Maggie Miller, "Russian Invasion of Ukraine Could Redefine Cyber Warfare," *Politico*, January 28, 2022: https://www. politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.

[132] Miller, "Russian Invasion."

[133] See Sean T Lawson, *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond* (London and New York: Routledge, 2020).

[134] Putin in: David Ignatius, "Russia's Radical Strategy for Information Warfare," *Washington Post*, 18 January 2017: https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/.

as a cyber puppet master, has arguably served Russia well, rendering the mere thought of Russia's capabilities into an influence operation in its own right.

In other words, the hypothesis suggests that expectations of Russian cyber capabilities are inflated and based on poor analysis, fuelled by Russian deception. However, some argue that expectations have failed because Russia has been withholding their heavy cyber artillery. Russia might thus still live up to expectations. Christopher Painter, the former cybersecurity coordinator at the State Department, is for example quoted as having said that Russia might be holding its most potent capabilities in reserve.[135] The US Senate Intelligence Chair, Mark Warner, reportedly suggested that "we have not [yet] seen their A-game tools."[136] Others add that the argument is nonsensical, since there would have been no better occasion to cripple Ukrainian civilian and military capabilities than in February last year.[137]

In conclusion, this hypothesis suggests that one of the reasons why those awaiting a destructive cyberwar or serious strategic results from cyberwarfare is that they might have set their expectations on Russian capabilities too high or that they have yet to be realised. In either case, Russia has not lived up to expectations.

4.2 Failed Capabilities

The second hypothesis concerns Russia's failure to achieve strategic effect in cyberspace; wrong expectations are not the same as failed capabilities. This hypothesis should be read against the background that Russia has been using Ukraine as a test lab for offensive cyber operations (see Chapter 3) and had an active presence in several Ukrainian networks during the run-up to the full-scale invasion.[138]

First, one argument suggests that since Russia was most likely expecting a short blitzkrieg invasion, Russian leaders had no intention of taking out critical infrastructure with cyber operations but of controlling the information environment and the Ukrainian population. In line with Russian strategy on irregular warfare, cyber operations were part of an influence campaign to polarise Ukrainian society and create distrust vis-à-vis the government. The "special operation" was meant to exploit tensions within Ukraine in order to overthrow the government and establish sustainable control of the country.[139] One of the likely reasons why this influence campaign did not take hold is the adverse effect, from a Russian perspective, of

---

[135] Painter in: Miller, *The World Holds*.

[136] Warner in: Miller, *The World Holds*.

[137] Nadiya Kostyuk and Erik Gartzke, "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," *Texas National Security Review* 5, no 3 (2022): 113–126, p 123–124.

[138] Willet, *The Cyber Dimension*, p 11.

[139] Štrucl, "Russian Agression," p 116.

the "special operation" on the Ukrainian people and their leadership, i.e., it provoked a massive national resistance and further increased the aversion to Russia, an aversion that not even the most clever cyber-enabled influence operations could change.

A related argument is that the Russian doctrinal and strategic focus on cyber operations, under the umbrella of information confrontation, leads to a suboptimal distribution of resources and development of capabilities. Moore argues, for example, that the "degree of finesse required to successfully influence mass global media is incomparable to disconnecting aircraft from their regional command."[140] Gavin Wilde reaches a similar conclusion. He suggests that by assessing Russian cyberwarfare through the lens of empathic strategy, "Moscow's information warfare thinking, its offensive cyber capabilities, and its organisational construct proved simply unfit for purpose in an event-driven, combined-arms campaign of the sort undertaken in February 2022."[141]

Yet another argument suggests that Russian leadership and operators committed strategic and tactical mistakes. Given their pre-positioning and reconnaissance in Ukrainian networks, they were well-prepared to launch offensive cyber operations. During the initial phase of the full-scale invasion, several such operations appear to have been launched. However, since the "special operation" was not planned to turn into a war of attrition, the Russian forces had no backup plan once their most potent means of attack had been attempted. This could explain why Russian APT actors conducted less sophisticated operations on less secure targets and reconnaissance after the initial phase of the invasion.[142]

Moreover, as Lin points out, earlier cyberattacks on Ukrainian critical infrastructure were carried out with significantly less comprehensive coordination than what a nationwide endeavour would call for. Conducting cyber operations within Ukraine itself, as opposed to primarily near the Russia-Ukraine border, would likely present greater coordination challenges, which contrasts with previous Russian operations that were largely localised to the border region.[143]

Another related argument is that Russian offensive cyber capabilities have failed in the same manner as the rest of the "special operation," the reason being Putin's restricting the plans of the full-scale invasion to a very limited circle.[144] Since preparation of presence-based and high-impact cyber operations is costly and time-

---

[140] Moore, *Offensive Cyber*, p 37.

[141] Wilde, "Cyber Operations," p 14.

[142] Vitiuk, interviewed in Alperovich and Gray, "How Russian."

[143] Lin, *Russian Cyber*, p 37.

[144] For a detailed discussion of Putin's path to war, see Owen Matthews, *Overreach: The Inside Story of Putin's War Against Ukraine* (London: Mudlark, 2022), p 153–182.

consuming, this suggests that the perceived need for strategic secrecy rendered Russian cyber capabilities unfit for the task. Martin, the former CEO of the UK's National Cyber Security Centre, is reported to have stated that "if, as seems to be the case, Putin withheld knowledge of his invasion plans from large sections of the Russian military and intelligence bureaucracy, then they wouldn't have had time to prepare those attacks, and you can't just conjure up a powerful cyberattack overnight."[145]

Finally, another argument is that it was a strategic mistake for Russia to ramp up its attacks against Ukraine after taking Crimea, since it made Ukraine aware of the importance of developing defensive capabilities and moved NATO and EU countries to start taking the Russian cyber threat seriously. Russia's mistake was thus to have revealed its cards too early.[146]

In sum, the failed-capabilities hypothesis suggests that Russia's offensive cyber capabilities have been strategically and tactically misdirected, in combination with poor planning and strategic secrecy.

4.3 Failed Analysis

Another hypothesis is that Russia is not performing as poorly as suggested, but that the analysis of Russia's cyber impact is flawed. It should be noted that none of the cited sources allude to cyber campaigns and operations as being able to bring about damage similar to that resulting from kinetic warfare.

In an early assessment, published in June 2022, Microsoft's President and Vice Chair, Brad Smith, stated that "the recent and ongoing destructive [Russian] attacks themselves have been sophisticated and more widespread than many reports recognise," adding that "the Russian army is continuing to adapt these destructive attacks to changing war needs, including by coupling cyberattacks with the use of conventional weapons."[147]

The Canadian Centre for Cyber Security made a similar early assessment: "the scope and severity of cyber operations related to the Russian invasion of Ukraine

[145] Martin, in Miller, *The World Holds*.

[146] Vitiuk, interviewed in: Alperovich and Gray, "How Russian."

[147] Smith, in *Defending Ukraine*, Microsoft, p 2. Smith and the Microsoft report were criticised for inflating the effect of cyberattacks during the initial phase of the war, some adding that this was due to economic self-interest. See Suzanne Smalley, "Cybersecurity experts question Microsoft's Ukraine report," *Cyberscoop*, 1 July 2022: https://cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/.

has almost certainly been more sophisticated and widespread than has been reported in open sources."[148] The Centre, moreover, stated that "Russian state-sponsored cyber-threat actors will almost certainly continue to perform actions in support of the Russian military's strategic and tactical objectives in Ukraine."[149]

David Cattler, NATO's Assistant Secretary-General for Intelligence and Security, and Daniel Black, Principal Analyst in NATO's Cyber Threat Analysis Branch, argue that the idea that Russia has failed in the cyberspace "is a dangerous misdiagnosis."[150] They concede that the evidence suggests that Russia had indeed orchestrated a coordinated cyber campaign to gain an early advantage in the conflict of an unprecedented scale, also arguing against those who claim that cyberwarfare has not contributed any strategic value. They conclude by stating that "cyber-operations have been Russia's biggest military success to date in the war in Ukraine."[151]

Moreover, commenting on the Viasat KA-SAT attack, a Ukrainian cyber-security official seemed to support these claims. The official was reported as stating that the takedown of the satellite caused "a really huge loss in communications in the very beginning of war."[152] This statement acquired wings and was spread in international news and social media, which led many to assume that the attack was a proof of concept of an offensive cyberattack's severely crippling military communications. It appears, however, that the official's quote was an answer to a hypothetical question. In other words, if the military had been using the satellite, it could have been devastating. But the military, who mainly rely on landlines, was not affected. In a follow-up interview, the official explained to journalist Kim Zetter that "it [the attack] had a serious impact on [the] satellite component of communications. But this is not the primary way of communications in armed forces. Landlines are the priority. And in case landlines were destroyed, that could be a serious issue in the first hours of war."[153]

---

[148] *Cyber Threat Activity Related to the Russian Invasion of Ukraine*, Canadian Centre for Cyber Security, Government of Canada, 2022, p 2: https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.

[149] *Cyber Threat Activity Related to the Russian Invasion of Ukraine*, Canadian Centre for Cyber Security, p 2.

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

[151] Cattler and Black, "The Myth."

[152] Quoted in: Raphael Satter, "Satellite Outage Caused 'Huge Loss in Communications' at War's Outset - Ukrainian Official," *Reuters*, 15 March 2022: https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/.

[153] Offical, in Kim Zetter, "Viasat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Official Says," *Zero Days*, 26 September 2022: https://www.zetter-zeroday.com/p/viasat-hack-did-not-have-huge-impact.

Referring to an article in the *Washington Post*, Zetter nevertheless stated that this "doesn't mean that Ukrainian military communications haven't been impacted during the conflict."[154] The article recounts the Battle for Kyiv. It references official sources within the Ukrainian Armed Forces, one of them stating that Russian forces jammed military communications and satellite networks, resulting in the "[m]ilitary communications [being] completely paralysed" in the Western parts of the city.[155] The article does, however, not reveal whether the jamming was achieved through cyber capabilities and/or electromagnetic warfare.

Another possibility less discussed in the literature is that Russia was close to succeeding with its "special operation." The authors of the aforementioned RUSI report on conventional warfare during the first six months of the full-scale invasion wrote that the Russian forces "came much closer to doing so [that is, succeeding in executing their plan] than is widely appreciated."[156] If Russia had succeeded in crippling the Ukrainian presidential administration, either by execution or displacement, capturing local officials, creating enough shock to prevent the Ukrainian population from mobilising, and disintegrating the Ukrainian civil society,[157] the assessment of the myth of Russia's overwhelming offensive cyber capabilities would perhaps have remained today. Moreover, the Russian strategy of controlling the information environment, either by knocking out Ukrainian communications or by taking them over, has not been an all-out failure.

For example, in late September 2022, a Ukrainian official reported that Russia had significantly damaged Ukraine's telecommunications infrastructure during the war with Russia. Approximately 4000 base stations of Ukrainian mobile-telephone carriers were damaged or taken over, along with tens of thousands of kilometres of fibre-optic communication lines. Additionally, 18 antenna masts used for broadcasting TV and radio signals were destroyed. Theft of Ukrainian frequencies for broadcasting Russian messages has also occurred. Equipment has been seized from Ukrainian companies to provide internet services on behalf of Russian media outlets.[158] Russian forces persistently attempt to link Ukrainian internet service providers to a system under their own control and overseen by their special services.

---

[154] Zetter, "Viasat Hack."

[155] See 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/.

[156] Zabrodskyi et al, *Preliminary Lessons*, p 12.

[157] Zabrodskyi et al, *Preliminary Lessons*, p 10.

[158] "Yurii Shchyhol: The Russian Federation Has Turned Even Communication Into a Weapon," State Service of Special Communications and Information Protection of Ukraine, 27 September 2022: https://cip.gov.ua/en/news/yurii-shigol-rosiiska-federaciya-peretvorila-na-zbroyu-navit-zv-yazok.

This is done to restrict access to Ukrainian online resources and achieve total control of the online activities of Ukrainian users. Many tactics have been used, including blackmail and intimidation, to compel compliance of those who resist collaboration with the Russian forces.[159] Coupled with these tactics, Russian actors had prepared a network of false local area and community channels on social media to provide a distorted picture of reality once these areas were occupied.[160]

Another argument is that at the outset of the full-scale invasion, Ukraine predominantly had to rely on older weaponry and systems with limited networking capabilities. This has made it harder for Russian actors to target the Ukrainian military through cyber operations. However, as Ukraine gradually integrates NATO equipment with sophisticated software and extensive networking, there's a possibility that Russia may intensify its cyber operations against an increasingly networked Ukrainian system.[161]

Finally, as mentioned, without complete and reliable data, it is impossible for an external actor to obtain the full picture. Catler and Black insist that, based on the available data, those who argue outright that cyberwarfare bears little to no relevance to the war appear to be misreading reality.[162] Ukrainian officials also communicate that, as of 2023, they are continually fending off exploits and attacks that are highly sophisticated, although not what they would call deadly cyber weapons.[163]

---

[159] "Invaders Use Blackmailing and Intimidation to Force Ukrainian Internet Service Providers to Connect to Russian Networks," State Service of Special Communications and Information Protection of Ukraine, 13 March 2022: https://cip.gov.ua/en/news/okupanti-shantazhem-i-pogrozami-zmushuyut-ukrayinskikh-provaideriv-pidklyuchatisya-do-rosiiskikh-merezh.

[160] Ksenia Ilyuk, Yevhen Sapolovich, and Ira Ryaboshtan, "'Now We Will Live to the Fullest!' How and Why Russia Has Created a Telegram Channels Network for the Occupied Territories of Ukraine," Detector Media, 5 May 2022: https://detector.media/monitorynh-internetu/article/199010/2022-05-05-now-we-will-live-to-the-fullest-how-and-why-russia-has-created-a-telegram-channels-network-for-the-occupied-territories-of-ukraine/.

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

[162] Catler and Black, "The Myth."

[163] See, for example, Philip Heijmans, "Ukraine Sees Russian Cyberattacks Growing More Sophisticated," *Bloomberg*, 24 October 2023: https://www.bloomberg.com/news/articles/2023-10-24/ukraine-sees-russian-cyberattacks-growing-more-sophisticated?embedded-checkout=true.

4.4 Successful Defence

Regardless of the absence of whether cyber shock and awe depends on an inflated understanding of Russia's offensive cyber capabilities, its failure in cyberspace, or a flawed analysis of the real impact of its cyber campaigns, many analysts and scholars emphasise that the characteristics of Ukraine's cyber defence and cyber security play a crucial role in understanding the role of cyberwarfare in the war.

First, given that hostile Russian cyber campaigns had already been targeting Ukraine for at least eight years before the full-scale invasion, Ukraine has been forced to develop solid defensive capabilities and resilient networks and systems. Willet states: "Arguably the biggest factor in Russia's cyber failure, however, has been Ukraine's own cyber-security expertise. While the Russians have picked up considerable know-how in operating on Ukrainian networks since 2014, by the same token the Ukrainians have learned a great deal about Russian cyber operations."[164]

In 2016, Ukraine tightened its laws on cyber criminality, adopted a National Cyber Security doctrine, and set up the National Cybersecurity Coordination Centre.[165] Apart from dealing with crime, the other critical areas they set as priorities included developing a safe and reliable cyberspace, securing government electronic information resources, safeguarding critical infrastructure, and developing cyber security capacity in the defence sector. For example, cyber hygiene courses are widely held and most public servants must pass a hygiene course.[166]

Moreover, intragovernmental, societal, and international cooperation were also highlighted as critical in 2016. As Oleksii Tkachenko, International Relations Officer in the Cyber Department of Ukraine's Security Service wrote in 2017, it was evident for Ukraine "that in order to address serious and persistent cyberattacks and threats, there is a need for enhanced collaboration at multiple levels – amongst national authorities, with the private sector and with international partners in order

[164] Willet, "The Cyber Dimension," p 16.

[165] In 2019, the Centre's mandate was further clarified and its capabilities expanded. For a more detailed discussion of Ukraine's cyber defence and security development, see Natalia Spînu, *Ukraine Cybersecurity: Governance Assessment*, Geneva Centre for Security Sector Governance (DCAF), 2020: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

[166] In terms of cyber hygiene, a free online course is available at governmental DIIA Education portal: "Basic Cyber Hygiene," Diia Education, accessed 16 October, 2023: https://osvita.diia.gov.ua/en/courses/cyber-hygiene.

to build the necessary capacities and respond effectively to such threats."[167] International cooperation involved, for example, the European Union and Council of Europe's project on cybercrime and the NATO Cyber Defence Trust Fund for defence. In addition, in 2020 the US Agency for International Development declared that it had invested USD 38 million in Ukrainian cybersecurity.[168]

Although many measures had been undertaken, in 2022 Ukraine still had apparent weaknesses.[169] Microsoft reported that, before the full-scale invasion, Ukraine had a Data Protection Law that prohibited government authorities from storing and processing data in public clouds. This meant that the digital infrastructure of the public sector operated on servers physically located within Ukraine. Recognising how vulnerable to potential missile or artillery attacks this setup was, Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, took action.

On 17 February 2022, Ukraine's Parliament amended the data protection law to permit government data to be moved from on-premises servers to the public cloud. This allowed critical government data to be relocated outside the country and stored in European data centres.[170] An immense data transfer followed. This involved the support of Amazon Web Services' so-called Snowball storage device,

[167] Oleksii Tkachenko, "Cybersecurity in Ukraine: National Strategy and International Cooperation," GFCE, 7 June 2017: https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/.

[168] Lin, "Russian Cyber," p 36.

[169] In 2020, in a report on Ukraine's cyber defence and security framework, Natalia Spînu concluded: "Ukraine lacks financial incentives to attract the best specialists to work for the government, and there is a sizable problem of cooperation between the public and private sectors, which is crucial for success in cybersecurity. Cyber is one of the fields that clearly demonstrates the interdependence of Ukraine."
See Spînu, *Ukraine Cybersecurity*, p 11. On measurements taken since the full-scale invasion and planned reforms, see "National Cybersecurity in the Context of the War: Main Achievements, Plans and Prospects," State Service of Special Communications and Information Protection of Ukraine, December 9, 2022: https://cip.gov.ua/en/news/nacionalna-kiberbezpeka-v-umovakh-viini-osnovni-dosyagnennya-plani-ta-perspektivi.

[170] Microsoft, *Defending Ukraine*, p 5.

an immense hard drive in a rugged suitcase. to move data out of the country physically.[171] Microsoft calls Fedorov's instinct "prophetic," since Russian missiles indeed targeted a Ukrainian government data centre at the beginning of the full-scale invasion.[172]

Other measures included instructing civilians, in particular in occupied areas, to use virtual private networks (VPN) and the TOR network to access Ukrainian websites and avoid Russian surveillance and targeting.[173]

An important addition is the resilience of Ukraine's ITC infrastructure. In 2019, Ukraine was ranked as having the 4th most reliable internet connectivity globally, and in 2022 the 6th most stable.[174] One important contribution factor is the fact that the end-user market in Ukraine does not have a dominant player or a single company that controls most of the market. This means that if one network experiences a problem or goes down, it does not significantly impact the entire network.

It is moreover important to note that most of the networks with many users in Ukraine are owned by Ukrainian companies. Over half of these networks serve less than 1% of the population. This creates a situation where many different options are available between these networks. They either directly connect or use Internet Exchange Points (IXPs) as intermediaries for connection.[175] In terms of physical infrastructure like cables, there is also a good level of resilience. There are multiple organisations providing services through diverse fibre paths. This diversity helps in maintaining a robust network. Where physical infrastructure has

[171] For more details, see Amazon Staff, "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; Russ Mitchell, "How Amazon Put Ukraine's 'Government in a Box'– And Saved Its Economy from Russia," *Los Angeles Times*, 15 December 2022: https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data.

[172] Microsoft, *Defending Ukraine*, p 5.

[173] See InMind, *Ukrainian Media Use and Trust in 2022*, USAID and Internews, 2022: https://internews.in.ua/wp-content/uploads/2022/11/USAID-Internews_Media-Consumption-Survey_2022_eng-1.pdf; Willet, "The Cyber Dimension."

[174] See Qrator Labs' annual ranking, "The National Internet Segment Reliability Research," *Medium*, 8 September, 2022: https://qratorlabs.medium.com/the-2022-national-internet-segment-reliability-research-60bd1278759b.

[175] An IXP is a hub where network operators peer and exchange traffic, serving as a foundational component of the internet but not providing complete connectivity like Internet Service Providers (ISP).

been damaged, Ukrainian network operators have been working efficiently to restore damaged infrastructure by cooperating with operators from competing companies.[176]

Against the above discussion, it comes as no surprise that, since the full-scale invasion, international support from the public-private sector has by many accounts played a crucial role in strengthening Ukraine.[177] Willet explains that many countries in the West have developed a growing cybersecurity industry based on tight collaboration between industry and government. For example, since early 2021, Microsoft has invested 239 million dollars in Ukraine and continuously supports the country by monitoring Russian cyber operations, while keeping the US government informed and supplying NATO and EU cyber experts with evidence of broader cyber activities.[178] Other companies, as discussed above, are Amazon and Google, as well as Cisco, Netnod, Truesec, and Recorded Futures. An informal group of volunteers, called the Cyber Defence Assistance Collaboration for Ukraine (CDACU), has also been launched.

It works together with the Ukrainian National Cybersecurity Coordination Centre by providing analysis and other forms of support.[179]

SpaceX's Starlink satellite-based internet system, whose costs as of mid-2023 are largely covered by the US,[180] is yet another example. During the early stage of the full-scale invasion, Ukraine's Minister of Digital Transformation, reached out to Elon Musk on Twitter to request Starlink services for stable communication amid widespread internet blackouts. Remarkably, within twelve hours, Musk responded affirmatively, activating Starlink services in Ukraine, and within two days new terminals were shipped to enhance connectivity. This rapid response benefited civilians and the military, with over 150,000 Ukrainians using Starlink by May 2022. Starlink became integral to Ukraine's infrastructure and military operations, even supporting unmanned aerial vehicles.[181] In early 2023, it was reported that SpaceX

[176] See Emile Alben, "The Resilience of the Internet in Ukraine," *RIPE Labs*, 10 March, 2022: https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine/.

[177] Lin, "Russian Cyber," p 36.

[178] Willet, "The Cyber Dimension," p 15.

[179] See: Voo, "Lessons from Ukraine's," p 18

[180] In October 2022, SpaceX communicated that the company would no longer be able to cover the costs for Starlink in Ukraine. In June 2023, the Pentagon announced that it had purchased satellite terminals for use in Ukraine. See: Amanda Macias and Michael Scheetz, "Pentagon awards SpaceX with Ukraine contract for Starlink satellite internet," *CNBC*, 1 June 2023: https://www.cnbc.com/2023/06/01/pentagon-awards-spacex-with-ukraine-contract-for-starlink-satellite-internet.html.

[181] "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" Belfer Center for Science and International Affairs, Harvard Kennedy School, 9 March 2023:

had started to limit the military use of Starlink with the argument that it was "never, never meant to be weaponised."[182]

Julia Voo notes that the "collaboration between the private sector and Ukraine demonstrates an unprecedented case of what is possible when there is an alignment of interests between a country at war and commercial technology companies with significant resources at their disposal and an interest in one side's victory."[183] However, the SpaceX episode also highlights the risk that a state entails when it becomes dependent on private entities for critical technology, despite its technical advantages.[184]

A final aspect of the successful defence hypothesis is that Ukraine, supported by allied states and hacker collectives, has succeeded in fending off Russia's offensive cyber operations by itself being offensive. The most illustrative case is when, two days after the full-scale invasion, the Minister of Digital Transformation announced on social media: "We are creating an IT army. We need digital talents."[185] The message contained information leading to a Telegram channel that came to function as a virtual base of operations. Two days later, the Ministry of Digital Transformation announced on its website: "We are also fighting on the cyber front. An IT army has been created for this purpose. These are talented specialists in the

---

https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.

[182] Dan Sabbagh, "Fury in Ukraine as Elon Musk's SpaceX Limits Starlink Use for Drones," *The Guardian*, 9 February 2023: https://www.theguardian.com/world/2023/feb/09/zelenskiy-aide-takes-aim-at-curbs-on-ukraine-use-of-starlink-to-pilot-drones-elon-musk. Although not a topic for this report, there is likely more to this story than has made it to the headlines of the major international news. Regulations on new ITC infrastructure in conflict and war create a complex legal landscape that needs further clarification. See for example, Matthew Fitzgerald and Cort Thompson, "What Does Starlink's Participation in Ukrainian Defense Reveal About U.S. Space Policy?" *Lawfare*, 26 April, 2022: https://www.lawfaremedia.org/article/what-does-starlinks-participation-ukrainian-defense-reveal-about-us-space-policy.

[183] Julia Voo, "Lessons from Ukraine's Cyber Defense and Implications for Future Conflict," in *Evolving Cyber Operations and Capabilities*, eds James A Lewis and Georgia Wood, Center for Strategic & International Studies, Washington, 2023, 15–22, p 18: https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities.

[184] This argument can also be made regarding strategic communication and the information environment, where platform X is an interesting case. During the initial phase of the full-scale invasion, X (then Twitter) appeared to have amplified Ukrainian messaging while restricting Russia's. After changes in company policies, presented as policies for freedom of information and freedom of speech, Russian messaging became less restrained and Ukraine has a harder time breaking through the noise of communication on the platform. See: Miah Hammond-Errey, "Elon Musk's Twitter Is Becoming a Sewer of Disinformation," *Foreign Relations*, 15 July 2023: https://foreignpolicy.com/2023/07/15/elon-musk-twitter-blue-checks-verification-disinformation-propaganda-russia-china-trust-safety/.

[185] Mykhailo Fedorov, Twitter [@FedorovMykhailo], 26 February 2022: https://twitter.com/FedorovMykhailo/status/1497642156076511233.

digital field: developers, cyberspecialists, designers, copywriters, marketers, targetologists. And not only Ukrainians! We receive help from all over the world. Everyone wishing from different countries join our army."[186] In the now typical humoristic style of Ukrainian strategic communications,[187] the Ministry added that "while Ukrainian cyber troops are working, Russian sites are down!"[188] Among its recent successful cyberattacks, presumably DDoS, it listed the Moscow Stock Exchange, government websites such as the FSB, Roskomnadzor, the President of the Russian Federation, and Russian news media sites such as Tass.

The foreign support alluded to in the Ministry's message appears to have come from, among others, hacker collectives such as the Belarusian Cyber Partisan, the Central and Eastern European Elves group, and Anonymous.[189] However, just as with the Russian hacker collectives' attacks and exploits in Ukraine, the effects of these attacks are hard to establish without further analysis. These groups likely also have an informational value.

The attack-as-defence policy does not seem restricted to Ukraine. In an interview on the historical and future role of hostile cyber activities in the Russo-Ukrainian war, Anne Neuberger, US Deputy National Security Adviser for Cyber and Emerging Technology, explained how the US practices cyber defence and security based on scenarios. One scenario, she explained, was to "ensure that we make it harder for attackers to conduct disruptive operations, whether that is disrupting infrastructure and more sensitive operations that I won't get into here."[190] As Lin concludes, this statement may indicate that "Western military or intelligence organisations

[186] "IT Army Blocks Russian Sites in a few Minutes – The Main Victories of Ukraine on the Cyber Front," Ministry of Digital Transformation of Ukraine, 28 February 2022: https://www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti.

[187] See: Ivar Ekman and Per-Erik Nilsson, *Ukraine's Information Front: Strategic Communication During Russia's Full-Scale Invasion*, FOI-R--5451--SE, Swedish Defence Research Agency (FOI), Stockholm, 2023: https://foi.se/rest-api/report/FOI-R--5451--SE.

[188] "IT Army Blocks," Ministry of Digital Transformation of Ukraine.

[189] Joel Schectman, Christopher Bing, and James Pearson, "Ukrainian Cyber Resistance Group Targets Russian Power Grid, Railways," *Reuters*, March 1, 2022: https://www.reuters.com/technology/ukrainian-cyber-resistance-group-targets-russian-power-grid-railways-2022-03-01/; Joe Tidy, "Meet the hacker armies on Ukraine's cyber front line," *BBC*, April 15, 2023: https://www.bbc.com/news/technology-65250356.

[190] Anne Neuberger in: Kara Swisher, "Are We Ready for Putin's Cyber War? I Asked One of Biden's Top Cybersecurity Officials," Sway (podcast), *The New York Times*, March 10, 2022: https://www.nytimes.com/2022/03/10/opinion/sway-kara-swisher-anne-neuberger.html?showTranscript=1.

may themselves have been conducting offensive cyber operations against Russian hackers to disrupt cyberattacks against Ukraine."[191]

In summary, the successful defence hypothesis contains at least three arguments. First, Ukraine has learned from being targeted by Russian hostile cyber operations for nearly a decade. Second, international support has been pivotal in preparing and defending Ukraine in cyberspace. Finally, offensive cyber campaigns and operations may have contributed to crippling Russia's offensive capabilities.

4.5 Conclusion

The analysis presented in this chapter revolves around several hypotheses concerning the effectiveness of Russia's cyber capabilities in its war against Ukraine. The *wrong expectations hypothesis* posits that overly optimistic assessments of Russian capabilities may have contributed to disappointment regarding the actual outcomes of cyberwarfare. According to this view, it is possible that the perceived potential of Russian cyberwarfare has not been realised as anticipated.

The *failed capabilities hypothesis* suggests that Russia's offensive cyber capabilities have suffered from strategic and tactical misdirection, compounded by inadequate planning and a lack of strategic transparency. This perspective contends that Russia may not have effectively leveraged its cyber assets, due to organisational and planning deficiencies.

The *failed analysis hypothesis* highlights that Russia's cyber operations have had an unparalleled historical impact. These operations have resulted in severe consequences, including instances of coordinated cyber and kinetic campaigns. It has been noted that Russia came close to achieving its initial goal of capturing Kyiv. While the nature of subsequent events remains speculative, it is suggested that this near-success may have prompted a reevaluation of analysts' and scholars' perceptions of Russia's information and cyber capabilities. Furthermore, it is anticipated that as Ukraine continues adopting increasingly sophisticated and interconnected technologies, it may potentially create additional vulnerabilities to offensive cyber operations. This underscores the dynamic nature of cyberwarfare and the imperative for conducting ongoing analysis and adaptation in response to evolving threats.

Conversely, the *successful defence hypothesis* contends that Ukraine's capacity to withstand cyber onslaughts rests on three key pillars. Firstly, Ukraine has accumulated invaluable experience over nearly a decade of being targeted by hostile Russian cyber operations, thereby learning to adapt and bolster its cyber defences throughout all of society. Secondly, international support has played a pivotal role in preparing and defending Ukraine in cyberspace, providing crucial resources and

[191] Lin, p 36.

expertise. Lastly, it is argued that the counteroffensive cyber campaigns mounted by Ukraine have succeeded in debilitating Russia's offensive capabilities, further strengthening Ukraine's defensive posture.

In evaluating these hypotheses, it is important to acknowledge that it may be premature to dismiss any of them entirely, particularly as they pertain to the evolving nature of cyberwarfare. In particular, Ukrainian authorities report continuous Russian activities and underscore the risk that threat actors might be waiting for the right moment to deploy attacks in already infected critical systems. However, the *successful defence hypothesis* holds particular weight, regardless of the validity of the other propositions.[192] The above assessment underscores the critical role of establishing baseline measurements and ensuring the reliability of data in assessing the true extent of Russia's cyber capabilities. While constructing a reasonable baseline without inflated expectations is certainly possible, the challenge, especially for external observers such as the present author, lies in accessing accurate and comprehensive data. Moreover, it is essential to consider the possibility that observed outcomes align with earlier and adjusted analyses of Russian cyber capabilities and cyberwarfare theory in general, reinforcing the need for a nuanced and multi-faceted understanding of this complex domain.

[192] Here, Nadiya Kostyk and Erik Gartzke would likely disagree, since they argue: "While numerous unobserved Russian cyber attacks might have been thwarted behind the scenes by Ukrainian (or other) cyber defenders, the attacks that have been observed are less of a reflection of Ukrainian excellence than of Russian lethargy; Russia's lack of preparation; or Russia's lack of a desire, need, or intent to execute disruptive and degrading cyber attacks." See: Kostyuk and Gartzke, "Why Cyber," p 123.

5 Adjusted Expectations

The four hypotheses presented above concern prior understandings of Russian and Ukrainian capabilities regarding the absence of cyberwar. The final hypothesis, adjusted expectations, is more theoretical and seeks to capture the thinking of analysts and scholars who argue that based on empirical evidence and theoretical knowledge of cyberwarfare, what we are seeing regarding Russia's full-scale invasion of Ukraine is more or less what is to be expected.

Lennart Maschmeyer and Natalia Kostyuk posed the perhaps most obvious question regarding the potential of cyberwarfare in an article published a couple of weeks before the full-scale invasion: "If cyber operations offer effective and potent instruments for coercion, why did Russia go to the effort and expense of mobilising its troops?"[193]

In an extensive analysis of cyber operations and theoretical literature, Daniel Moore concludes that offensive cyber operations are "a set of capabilities that act as a force multiplier in armed conflict" that does "not supplant but rather complement existing military doctrine."[194] In a similar study, Lucas Kello stated in 2018 that "there has never been, and possibly never will be, a true act of cyberwar."[195] He argued that "as far we can tell, malware is a largely ineffective tool of military victory. Cyberattack can augment but not replace traditional military power."[196] In 2012, regarding the theories of a "cyber Pearl Harbor," Thomas Rid concluded: "Unless significantly more evidence and significantly more detail are presented publicly by more than one agency, we have to conclude that there will not be a Pearl Harbor of cyberwar in the future either."[197]

The adjusted expectations hypothesis is discussed in more detail in this final chapter, focusing on operational restraints and strategic effect questions. The chapter also serves as the report's concluding discussion.

---

[193] Lennart Maschmeyer and Nadiya Kostyuk, "There is no Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict," War on the Rocks, 8 February 2022: https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

[194] Moore, *Offensive Cyber*, p 6.

[195] Kello, *The Virtual Weapon*, p 121.

[196] Kello, *The Virtual Weapon*, p 121.

[197] Rid, *Cyber War*, p 29.

5.1 Constraints

In the research literature, general constraints regarding the effect of cyberattacks have been discussed for decades. Max Smeets argues for example that inducing an arbitrary cyber effect on a system or network in an unplanned manner and devoid of discernible strategic intent is comparatively uncomplicated. Conversely, he argues, coordinating a meticulously calibrated cyber effect at a predetermined juncture, imbued with a distinct strategic aim that surpasses potential adverse repercussions, constitutes a formidable undertaking.[198]

Maschmeyer identifies three interrelated challenges, a "trilemma": the effort involved in turn reduces the plausibility of accomplishing successful high-impact cyberattacks; its three key variables are speed, intensity of effects, and control.[199] Firstly, he argues, the very effort involved slows down the speed at which operations produce their intended effects. Secondly, the effort limits the intensity of these effects, which depends on both the severity of the impacts on individual targets (referred to as "scope") and the overall societal impact, determined by the number of targets affected (referred to as "scale"). Thirdly, the efforts required to maintain secrecy and exploit systems can restrict control over the targeted system and its effects. The core of the trilemma is that improvements in one aspect tend to come at the cost of the other two, a negative correlation, in other words. For instance, if operational speed is increased, it often leads to decreased intensity and control.[200]

Maschmeyer adds that while there are expectations that advanced technology will enable lightning-fast cyber operations with widespread societal consequences under a shroud of secrecy, this trilemma makes the achievement of all these characteristics simultaneously exceedingly challenging.[201] As a result, in most cases, cyber operations fall short of their anticipated strategic potential and offer, at best, only limited strategic value.[202]

In terms of warfare, another constraint regarding cyberattacks is how they differ from kinetic attacks. The effect of a kinetic weapon is relatively direct, primarily determined by the potency of the payload, and not significantly influenced by the specific target. Cyberattacks, and cyber operations in general, differ, since they are target-dependent. A successful cyber operation depends both on the capability of

---

[198] Smeets, *No Shortcuts*, p 34.

[199] Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," International Security 46, no. 2 (2021): 51–90, p 55.

[200] It should be noted that this trilemma is not exclusive for cyberwarfare.

[201] Maschmeyer, "The Subversive Trilemma," p 55.

[202] This conclusion is also repeated in Maschmeyer's and Cavelty's analysis of cyberwarfare in Ukraine. See: Maschmeyer and Cavelty, "Goodbye Cyberwar," p1.

the threat actor and the vulnerabilities in the target. As Lin Herbert points out, "in contrast to kinetic weapons, the weapons and capabilities of offensive cyber operations are often customised in detail to the specific target(s) against which these operations may be directed, particularly when precision of attack is needed (for example, to minimise collateral damage)."[203] This means that "'off the shelf' weapons and capabilities to support offensive cyber operations are far less readily available than is the case for their kinetic counterparts."[204]

Yet another aspect of the relation between kinetic and cyber operations is their potential for combination. In a recent study, Nadiya Kostyuk and Erik Gartzke examined to what degree cyber operations are complements or substitutes to conventional, kinetic warfare in 2000–2010.[205] They conclude that "cyber neither triggers or substitutes for conventional conflict behaviour," instead "cyber conflict exists at present largely independently from conventional military operations."[206] When using their results to evaluate the role of offensive cyber operations in the Russo-Ukrainian war, they argue that the operations are best understood as an indirect substitute for conventional warfare: "Given that information campaigns are meant to shape public opinion in the long term, the Russian government might have been using these campaigns to indirectly substitute for fighting in the future."[207]

Finally, related to Maschmeyer's trilemma, the inherent complexity in developing potent cyberattacks, and the difficulties in combining cyber operations with kinetic operations is due to the human factor. For example, planning cyber operations from the strategic to the tactical levels involves people at every stage, e.g., a diverse and multidisciplinary workforce consisting of technicians, legal experts, data and security policy analysts, language experts, and front-office support persons. This reality is coupled with organisational questions, such as allocating resources and creating structures that facilitate and leverage human capability.[208] Thus, effectively orchestrating cyber operations proves to be a formidable challenge, as it necessitates the seamless integration of a diverse, multidisciplinary team alongside strategic resource allocation and structural optimisation, a task that is not always easily realisable.

---

[203] Lin, *Russian Cyber*, p 39.

[204] Lin, *Russian Cyber*, p 39.

[205] Nadiya Kostyuk and Erik Gartzke, "Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations," *Journal of Conflict Resolution*, online first (2023): 1-28.

[206] Kostyuk and Gartzke, "Fighting in Cyberspace," p 22.

[207] Kostyuk and Gartzke, W*hy Cyber*, p 122.

[208] Smeets, *No Shortcuts*, p 7.

Yet another aspect of the human factor in cyber operations is presented by workload and stress. In a study engaging a cohort of 126 cyber operators within the US National Security Agency, Josiah Dykstra and Celeste Lyn Paul found that the dynamics of a high-stakes environment characterised by a confluence of complex tasks exacts a toll on human operators. Based on a scrutiny of earlier results, they conclude that negative effects related to a demanding cognitive workload, such as operator fatigue, frustration, risk for errors, diminished performance, and burnout, increased throughout an operation.[209]

Taking these constraints into consideration, it is not surprising that the Russo-Ukrainian war is not the proof of concept of a full-scale cyberwar that some have speculated on. However, as underscored earlier, this does not mean that cyberwarfare is negligible in contemporary war.

Pondering the "expectations-reality" debate in September 2023, Chris Painter, the first coordinator of cybersecurity issues at the US State Department, from 2009 to 2017, stated that "I think part of it were the expectations were never realistic, that cyber would be the deciding factor in a physical war. That was never going to be true, and I think it's--you know, I think we're a victim of our own hype in that sense."[210] Painter is adamant, however, in pointing out that if expectations are adjusted to previous experiences, then "it's playing the role I think we should expect it to play, and I think the wrong lesson to draw is that cyber didn't bark, and therefore, it's not that important an issue, because it's playing a critical integrated role, as you'd expect in any conflict."[211]

5.2 Effect and Value

While numerous scholars and analysts concur on delineating the constraining elements within cyber operations, their assessments of the resultant impacts of the operations exhibit a lack of uniformity.[212]

Some argue that cyber operations offer little to no strategic value or effect and their capabilities are hard to integrate into multidomain warfare. For example, Maschmeyer and Cavelty state that a "sober look at the evidence shows that cyber operations are

[209] Josiah Dykstra and Celeste Lyn Paul, "Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations," *Journal of Information Warfare* 16, no 2 (2017): 1–11.

[210] Painter, in "Transcript: Securing Cyberspace: Next Generation of Threats," *Washington Post*, 26 September 2023: https://www.washingtonpost.com/washington-post-live/2023/09/26/transcript-securing-cyberspace-next-generation-threats/.

[211] Painter, in "Transcript: Securing."

[212] For a more in-depth discussion, see Bateman, "Russia's Wartime."

either too slow, weak, or volatile to serve as attack tools in military operations. Even in hybrid settings, they offer limited strategic value."[213]

Others, such as Painter, argue that while cyberwar is an exaggeration, cyberwarfare is still powerful in integrated warfare. Thus, the question here does not pertain to the realm of cyberwarfare, which is often regarded as an improbable scenario. Rather, the focus lies on whether, within the framework of the adjusted expectations hypothesis, offensive cyber activities offer a potential contribution to the broader landscape of warfare.

This begs the question of what we mean by strategic value and effect. Maschmeyer and Cavelty do not define strategic value explicitly, but appear to equate it with "catastrophic attacks."[214] The present report discusses a strategic advantage in terms of its having a favourable position or condition that helps one side in a conflict achieve its goals more effectively than the other. This advantage can come in different forms, such as better positioning, intelligence, logistics, technology, or overall strategic planning. It gives one side the advantage of more control throughout the conflict and increases its chances of attaining the desired outcomes. Functional capabilities that lead to a strategic advantage arguably have a strategic value and effect, even if these capabilities in themselves are not "catastrophic."

When considering the strategic effect and value of cyberwarfare in isolation, it is improbable that it should be simply equated to mere cyber vandalism. As highlighted by Smeets and Gartzke, the fundamental problem lies in attempting to assess the potential of cyberwarfare as a definitive determinant in conflict resolution. Such an evaluation is inappropriate when applied to cyberwarfare and a criterion that very few, if any, warfare capabilities would meet.[215]

For instance, when viewed as a decisive determining factor, it can be contended that Russian conventional warfare has not yielded the intended strategic impact either. The anticipated results of the "special operation" have not materialised; the initial plan faltered, resulting in increased national cohesion within Ukraine rather than division. Furthermore, the war has led NATO to demonstrate increased cohesion and resolute support for Ukraine rather than creating division among the alliance's member countries. However, while this is the current status at the time of writing, the war is far from over and evaluating strategic effects before the fact is likely premature.

---

[213] Maschmeyer and Cavelty, "Goodbye Cyberwar," p 1.

[214] The closest they come to a definition is "The reason is an operational trilemma that constrains the speed, intensity, and control that cyber operations can achieve – thus limiting their strategic value and rendering catastrophic attacks highly improbable." See Maschmeyer and Cavelty, "Goodbye Cyberwar," p 1.

[215] See Smeet's discussion, based on Gertzke, in Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no 3 (2018): 90–113, p 92–93.

In understanding and assessing the strategic effect and value of hostile cyber activities, much as in relation to the constraints of cyber operations, the human element plays a pivotal role, as emphasised by various scholars. In short, cyberwarfare transcends isolated technological pursuits. Ultimately, all attacks target the human factor rather than mere technology. Gartzke and Kostyuk argue, for example, that "cyberwar is more about beliefs and data than it is about wresting physical control over objects or destroying material capabilities."[216]

As Martin Libicki suggests, gaining a strategic advantage through cyber operations is not solely an engineering matter;[217] it hinges on how a specific cyber operation interfaces with and influences other domains of warfare, as well as military and political decision-making.[218]

Discussing the topic of effect within the realm of cyberwarfare, Smeets distinguishes between two capabilities: counterforce and countervalue.[219] Counterforce pertains to offensive cyber capabilities directed at targets relevant to military operations, while countervalue targets the adversary's vital assets.[220] These vital assets pertain to broader psychological, societal and political dynamics. Indeed, recent research indicates, for example, that cyberattacks induce levels of psychological distress comparable to conventional acts of terrorism and political violence, challenging the one-sided focus on material effect.[221] In other words, a deeper understanding of the correlation between effects in cyberspace and the domain is needed.

---

[216] Kostyk and Gartzke, "Why Cyber," p 123.

[217] Libicki, however, contends that engineering is still a central part of cyberwarfare: "Cybersecurity sits at the uncomfortable intersection between engineering and conflict. Winning a conflict is not the same as solving an engineering problem, largely because the other side never stops evolving to frustrate the engineering. The fact that attackers cannot get into one's system except through paths already extant in the system, however, suggests that engineering has a stronger role to play in modulating cyber conflict than in modulating physical conflict." See Martin Libicki, *Cyberspace in Peace and War* (Annapolis: Naval Institute Press: 2021), ch 4:8, para 8.

[218] To evaluate military offensive cyber operations, Moore proposes a cumulative analysis of five parameters: 1) target (quality or quantity); 2) impact (both initially, which often shows little or no physical effects, and, because of this, the wider, long-term observable consequences); 3) attacker (establishes attribution to a state or substate entity); 4) goals (assessing degree of a military-strategic agenda); 5) relationships (larger geopolitical and strategic circumstances of the attack, key in assessing warfare or other adversarial situations). See: Moore, *Offensive Cyber*, p 16.

[219] Smeets, "The Strategic Promise."

[220] Smeets, "The Strategic Promise," p 94.

[221] See Ryan Shandler, Michael L. Gross, and Daphna Canetti, "Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis," *Journal of Global Security Studies* 8, no 1 (2022): 1–19.

Travis Sharp illuminates the societal and political effects and strategic value of hostile cyber activities. In recent history, Russian cyber operations have, for example, proved quite capable of inflicting damage to the social and political fabric of the US The hack-and-leak operation against Hillary Clinton's presidential campaign, in 2016, led to "questions about the integrity of the Democratic Party's presidential-nominating process" that,[222] in relation to Donald Trump's alleged collusion with Russian intelligence, drove a wedge into the reliability of the democratic process of the country. Sharp argues that "leaders of democracies may be especially vulnerable since embarrassing disclosures cause media and political frenzies that they cannot suppress."[223] In a wartime scenario, such disclosures can prove harmful, potentially eroding trust within the population and precipitating significant blows to morale. This example shows the potency, either direct or indirect, as an enabler of influence operations that, arguably, are strategic.

Against the backdrop of the Russo-Ukrainian conflict, attaining strategic success hence extends beyond the execution of effective cyber operations. It encompasses considerations that are beyond immediate battlefield consequences and worst-case scenarios, and delving into the enduring effects on the human element within the military, politics, and society. Even if cyber operations may not entail the extreme scenario of a cyber Armageddon, they can gradually erode vital capabilities or lead to significant impacts extending beyond the realm of material assets. However, the inherent unpredictability of human responses significantly complicates forecasting the outcomes of large-scale successful cyber operations. Unlike automated processes, human reactions to such events can vary widely and are challenging to forecast. For instance, a major cyberattack, akin to an act of war, might not always yield the intended weakening effect on the targeted nation. Instead, it could potentially foster a sense of societal unity and resolve within the affected country. As is the case in Ukraine, this strengthened internal solidarity have been accompanied by increased international support. Thus, effective cyberattacks could counterintuitively bolster the resilience of the targeted state. Such dynamics underscore the critical role of the human element in shaping the aftermath of cyber operations, making their consequences less predictable and more complex to anticipate.

[222] Travis Sharp, "Hiding in Plain Sight: Political Effects of Cyber Operations," *Survival 60*, no 6 (2018): 45–53, p 48.

[223] Sharp, "Hiding in Plain," p 48.

5.3 Conclusion

This chapter discusses the last of our five hypotheses – adjusted expectations – concerning the capabilities of Russia and Ukraine in the context of cyberwarfare. The hypothesis is more theoretical than the other four and suggests that, based on empirical evidence and theoretical knowledge of cyberwarfare, the extent of its role in Russia's full-scale invasion of Ukraine is in alignment with what can be reasonably anticipated.

The adjusted expectations hypothesis revolves around operational limitations (constraints) and questions about strategic impact (effect and value). Constraints on the effectiveness of cyberattacks have been a subject of discussion in the research literature for quite some time. Smeets argues, for example, that executing a cyber effect without discernible strategic intent is relatively straightforward, but orchestrating a meticulously calibrated cyber effect with a specific strategic aim, while mitigating potential adverse repercussions, is a formidable challenge. Maschmeyer identifies a "trilemma" that comprises speed, intensity of effect, and control, diminishing the feasibility of successful high-impact cyberattacks. Improving one aspect of the three often comes at the expense of the other two, illustrating the complex trade-offs involved. Moreover, the human element adds complexity to the execution of cyber operations, requiring seamless coordination among a diverse team and strategic resource allocation. Additionally, workload and stress further compound the challenges that offensive and defensive cyber operators face.

Considering these constraints, it becomes evident that the Russo-Ukrainian war is not a definitive proof of concept for a full-scale cyberwar. Nonetheless, this does not diminish the significance of cyberwarfare in contemporary and future conflicts. While it seems clear that the conduct of cyber operations as a final arbiter of war, or as a single domain enterprise, will not be feasible in the near future, if ever, there is no consensus regarding the potential of hostile cyber operations as a complement to regular warfare. Kostyuk and Gartzke demonstrate the complexity of integrating cyber operations in conventional warfare and that this has rarely happened. However, in a time of rapid technological development and the integration of the cyber domain in virtually all aspects of human life, their analysis is based on old data.

The contention here is that an analysis of the Russo-Ukrainian war illustrates that cyberwarfare indeed appears to be one of its crucial elements, both in carrying out cyber-enabled influence operations, and on the battlefield, for targeting and taking out communications. While an in-depth analysis of the countereffect of Russian cyber operations is needed, there is now a lack of publicly available data, a situation that will likely continue throughout the war. Regardless, if cyberwar cannot be seen as a single domain for interstate war, and cyberwarfare is understood as only a force multiplier, then it will be incorrect to evaluate cyber campaigns and operations in isolation. The broader impact regarding countervalue is essential in understanding the potential of hostile cyber activities, both in the context of war and unpeace. Even if a cyberwar is a long-lived "myth," as Erik Gartske argues, it would be wrong "to

infer that there is no role for the Internet in twenty-first-century conflict."[224] Gartzke continues, "[indeed, the real message for soldiers and politicians is that cyberwar involves a broadening of the dimensions of warfare, rather than a narrowing of future conflict."[225] As Moore concludes: "The historical lessons from cyber-warfare are therefore that its true uniqueness stems from its unprecedent reach, sophistication, and scope, not from truly being a new domain of warfare."[226]

Drawing conclusive lessons learned that are based on how hostile cyber activities have been used since Russia's full-scale invasion is premature. The hypotheses discussed in this report should be appropriately correlated as more data becomes available for public analysis. While this report, as well as the publications of many of the scholars and analysts quoted here and elsewhere, urges basing future research on empirical data and real-world events, this does not imply that speculative and creative thinking regarding future threats in the cyber domain has no place. When working with lessons learned within the military context, ages-old wisdom pertains to the cyber domain. To paraphrase Mike Dana: the military trains for the past war, not the future war.[227] This conveys that military forces often prepare and train on the basis of the experiences and tactics of previous conflicts rather than on anticipation of the unique challenges of future, potentially unforeseen conflicts. This sentiment underscores the importance of being receptive to rapid technological developments and vulnerabilities that emerge in an ever-expanding and interconnected cyber-space.

It is imperative to assess hostile cyber operations within their distinct contexts. Primarily, in the case of Russia and Ukraine, a state of war has persisted since 2014. Therefore, employing the analytical framework represented by the notion of cyberwarfare is well-suited for comprehending this scenario. Nonetheless, when examining offensive Russian cyber activities beyond the borders of Ukraine, it is vital to recognise them as occurring in a situation characterised by unpeace. In conclusion, it is worth noting that another country subjected to a similar cyber onslaught as Ukraine may not be as resilient. This implies that theoretical insights from cyberwarfare studies, as well as their applicability to other nations, should be approached with caution.

Finally, any reading of this report as concluding that Russian cyberwarfare and hostile cyber activities in general pose no tangible threat is wrong. On the contrary, downplaying the threat posed in the cyber domain would likely be a grave mistake.

---

[224] Erik Gartzke, "The Myth of Cyberwar," p 538.

[225] Gartzke, "The Myth of Cyberwar," p 538.

[226] Moore, *Offensive Cyber*, p 67.

[227] For further discussion, see: Mike Dana, "Future War: Not Back to the Future," *War on the Rocks*, 6 March 2019: https://warontherocks.com/2019/03/future-war-not-back-to-the-future/.

6 Summary

This report has sought to provide an analysis of the role of cyberwarfare in the Russo-Ukrainian war, aiming to derive key learnings and conclusions about its impact and effectiveness. The report covers several vital aspects of cyberwarfare, integrating theoretical approaches with empirical data to offer a comprehensive understanding of this modern warfare domain.

The first chapter delves into the conceptual framework of cyberwarfare. It differentiates between 'cyberwar' and 'cyberwarfare,' underscoring the relevance of the latter in armed conflict scenarios. The report also introduces the term 'unpeace' to describe the evolving dynamics of cyberspace, which is particularly relevant in the context of the Russo-Ukrainian war. Additionally, a hierarchy of cyber activities is established, categorizing them from cyber campaigns to cyberattacks in terms of complexity and impact.

The subsequent chapter evaluates Russia's cyber activities in Ukraine from 2014 to 2023. These activities range from basic to advanced operations, with varying strategic values. The analysis includes the examination of the strategic value of these operations, especially in the context of the annexation of Crimea and the full-scale invasion in 2022. The potential strategic value of these operations in multidomain warfare is discussed, with a focus on the correlation and causation with kinetic operations.

Further, the fourth chapter explores various hypotheses explaining the role of hostile Russian cyber activities during the war. These include the Wrong Expectations Hypothesis, suggesting an overestimation of Russian cyber capabilities; the Failed Capabilities Hypothesis, pointing to potential weaknesses in Russia's cyber strategy; the Failed Analysis Hypothesis, which argues for a re-evaluation of Russian cyber operations' impact; and the Successful Defence Hypothesis, highlighting Ukraine’s resilience against cyber onslaughts. The analysis suggests that while it is premature to dismiss any of these hypotheses, the successful defence hypothesis holds particular weight.

The final section discusses the ‘Adjusted Expectations’ hypothesis, proposing that Russia’s cyber activities align with empirical evidence and theoretical knowledge. It emphasizes the importance of strategic intent in evaluating cyberwarfare effectiveness and acknowledges the complexity added by the human element in cyber operations. The report concludes that the Russo-Ukrainian war is not a definitive proof of concept for full-scale cyberwar but highlights the significant role of cyberwarfare in contemporary conflicts. The necessity for vigilance in cyberspace and the importance of resilience against cyber threats are underscored.

In light of the evolving landscape of cyberwarfare, as vividly illustrated by the Russo-Ukrainian war, the imperative for ongoing empirical research cannot be over-

stated. As more data becomes publicly available, it is crucial to continuously scrutinize and learn from these cyber activities. Equally important is the collaboration with practitioners in Ukrainian cybersecurity, whose frontline experiences offer invaluable insights. Together, these efforts will not only deepen our understanding but also enhance our preparedness and response to the ever-changing dynamics of cyber threats in the modern world.

7 References

"'Anonymous Sudan': Most Likely Russia Attempting to Disrupt Sweden's NATO Application." Truesec, February 20, 2023: https://www.truesec.com/-news/anonymous-sudan-most-likely-russia-disrupting-swedens-nato-application.

"Basic Cyber Hygiene." Diia Education, accessed 16 October, 2023: https://osvita.diia.gov.ua/en/courses/cyber-hygiene.

"Internet Crime Report Center Releases 2022 Statistics." *Federal Bureau of Investigation,* Springfield, March 22, 2023: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics.

"Invaders Use Blackmailing and Intimidation to Force Ukrainian Internet Service Providers to Connect to Russian Networks." State Service of Special Communications and Information Protection of Ukraine, March 13, 2022: https://cip.gov.ua/en/news/okupanti-shantazhem-i-pogrozami-zmushuyut-ukrayinskikh-provaideriv-pidklyuchatisya-do-rosiiskikh-merezh.

"IT Army Blocks Russian Sites in a few Minutes - The Main Victories of Ukraine on the Cyber Front." Ministry of Digital Transformation of Ukraine, February 28, 2022: https://www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti.

"National Cybersecurity in the Context of the War: Main Achievements, Plans and Prospects." State Service of Special Communications and Information Protection of Ukraine, December 9, 2022: https://cip.gov.ua/en/news/-nacionalna-kiberbezpeka-v-umovakh-viini-osnovni-dosyagnennya-plani-ta-perspektivi.

"Satellite Images Show Military Buildup in Russia, Ukraine." *Radio Free Europe and Radio Liberty*, April 21, 2021: https://www.rferl.org/a/russia-ukraine-military-buildup-satellite-images/31214867.html.

"Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" Belfer Center for Science and International Affairs, Harvard Kennedy School, March 9, 2023: https://www.belfercenter.org/-publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.

"Transcript: Securing Cyberspace: Next Generation of Threats." *Washington Post*, September 26, 2023: https://www.washingtonpost.com/washington-post-live/2023/09/26/transcript-securing-cyberspace-next-generation-threats/.

"Russians Struck at Kyiv TV Tower." Ukraine Institute of Mass Information, 1 March, 2023: https://imi.org.ua/en/news/russians-struck-at-kyiv-tv-tower-i44122.

"Update: Destructive Malware Targeting Organizations in Ukraine." Cybersecurity & Infrastructure Agency, United States Government, April 28, 2022: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a;

"Yurii Shchyhol: The Russian Federation Has Turned Even Communication Into a Weapon." State Service of Special Communications and Information Protection of Ukraine, September 27, 2022: https://cip.gov.ua/en/news/yurii-shigol-rosiiska-federaciya-peretvorila-na-zbroyu-navit-zv-yazok.

Alben, Emile. "The Resilience of the Internet in Ukraine." *RIPE Labs*, 10 March, 2022: https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine/.

Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations. Edition A Version 1, NATO, January, 2020.

Anonymous Sudan: Threat Intelligence Report. Truesec, Stockholm, 2023: https://www.truesec.com/hub/report/anonymous-sudan-threat-intelligence-report.

Cyber Threat Activity Related to the Russian Invasion of Ukraine. Canadian Centre for Cyber Security, Government of Canada, 2022, p 2: https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.

Joint Publication 3-12: Cyberspace Operations. US Joint Chiefs of Staffs, June 8 2018.

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

Russia's Cyber Tactics: Lessons Learned 2022. State Service of Special Communications and Information Protection of Ukraine, Kyiv, 2023: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine.

Alperovich, Dmitri and Patrick Gray. "How Russian Intelligence Operatives Have Attacked Ukraine in Cyberspace: Interview with the Security Service." *Geopolitics Decanted*, 21 August 2023.

Amazon Staff. "Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future." Amazon, 9 June 2022: https://www.aboutamazon.com/-news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

Antoniuk, Daryna. “Russia’s Turla hackers target Ukraine’s defense with spyware.” *The Record: Recorded Future News*, July 19, 2023: https://therecord.media/turla-hackers-targeting-ukraine-defense.

Azad, Tahir Mahmood, Muhammad Waqas Haider, and Muhammad Sadiq. “Understanding Gray Zone Warfare from Multiple Perspectives.” *World Affairs* 186, no. 1 (2023): 81-104.

Backman, Sarah. *Making Sense of Large-scale Cyber Incidents: International Cybersecurity Beyond Threat-based Security Perspectives* (Stockholm: Stockholm University, 2023).

Bateman, Joe. “Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.” Working Paper, Carnegie Endowment for International Peace, Washington, 2022: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

Black, James, Diana Dascalu, Megan Hughes, and Ben Wilkinson. *Strategic Advantage: Definitions, Dynamics, and Implications*. RAND Europe, RAND Corporation, Santa Monica and London, 2023: https://www.rand.org/-pubs/research_reports/RRA1959-1.html.

Brito, Jerry and Tate Watkins. “Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy.” *Harvard National Security Journal* 3 (2011): 1-39.

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

Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge and London: Harvard University Press, 2020.

Cattler, David 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.

Cherepanov, Anton. *WIN32/Industroyer: A New Threat for Industrial Control Systems*. ESET, 2017: https://web-assets.esetstatic.com/-wls/2017/06/Win32_Industroyer.pdf.

Chivvis, Christopher S. *Understanding Russian “Hybrid Warfare” and What Can be Done About It.* RAND, Santa Monica, 2017: https://www.rand.-org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

Clarke, Richard A and Robert K Knake. *Cyber War: The Next Threat to National Security, and What to Do About It*. New York: HarperCollins, 2010.

Courtney, William and Peter A Wilson. "If Russia Invaded Ukraine." *The Rand Blog*, December 8, 2021: https://www.rand.org/blog/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html.

Cyber Peace Institute. Data and Methodology. Accessed September 17, 2023: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology.

Cyber Peace Institute. Impact. Accessed September 17, 2023: https://cyberconflicts.cyberpeaceinstitute.org/impact.

Cyber Peace Institute. Ukraine Platform. Accessed September 17, 2023: https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

Dana, Mike. "Future War: Not Back to the Future." *War on the Rocks*, March 6, 2019: https://warontherocks.com/2019/03/future-war-not-back-to-the-future/.

Digital Security Unit. *Special Report: Ukraine - An Overview of Russia's Cyberattack Activity in Ukraine*. Microsoft, 2022, p 12: https://query.-prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Dinstein, Yoram. *War, Aggression, and Self-Defence*. Cambridge and New York: Cambridge University Press, 2017.

Dykstra, Josiah and Celeste Lyn Paul. "Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations." *Journal of Information Warfare* 16, no. 2 (2017): 1–11.

Ekman, Ivar and Per-Erik Nilsson. *Ukraine's Information Front: Strategic Communication During Russia's Full-Scale Invasion*. FOI-R--5451--SE, Swedish Defence Research Agency (FOI), Stockholm, 2023: https://foi.se/-rest-api/report/FOI-R--5451--SE.

Elkus, Adam. "50 Shades of Gray: Why the Gay War Concepts Lacks Strategic Use." *War on the Rocks*, December 15, 2015: https://warontherocks.com/-2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/.

Ericson, Marika. *On the Virtual Borderline: Cyber Operations and their Impact on the Paradigms for Peace and War*. Uppsala: Uppsala University, 2020.

Erickson, Jeff. "The Possibility Of A Cyber Pearl Harbor Remains Real, Says Former CIA Director." *Forbes*, March 13, 2019: https://www.forbes.com/-sites/oracle/2019/03/13/the-possibility-of-a-cyber-pearl-harbor-remains-real-says-former-cia-director/?sh=5a46a50859fb

Fedorov, Mykhailo. Twitter [@FedorovMykhailo], February 26, 2022: https://twitter.com/FedorovMykhailo/status/1497642156076511233.

Fitzgerald, Matthew and Cort Thompson. “What Does Starlink’s Participation in Ukrainian Defense Reveal About U.S. Space Policy?” *Lawfare*, 26 April, 2022: https://www.lawfaremedia.org/article/what-does-starlinks-participation-ukrainian-defense-reveal-about-us-space-policy.

Fruhlinger, Josh. “Petya ransomware and NotPetya malware: What you need to know now.” CSO, October 17, 2017: https://www.csoonline.com/-article/3233210/ransomware/petya-ransomware-and-not petya-malware-what-you-need-to-know-now.html.

Gartzke, Erik. “The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (2013): 41–73.

Giles, Keir. “Putin Does not Need to Invade Ukraine to Get His Way.” *Chatham House*, December 21, 2021: https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.

Givens, Austen. “Putin’s Cyber Strategy in Syria: Are Electronic Attacks Next?” *Cyber Defense Review*, November 17, 2015: https://cyberdefensereview.-army.mil/CDR-Content/Articles/Article-View/Article/1136170/putins-cyber-strategy-in-syria-are-electronic-attacks-next/.

Google. *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*. Mountain View: Google Inc, 2023: https://services.google.com/-fh/files/blogs/google_fog_of_war_research_report.pdf.

Gordon, Michael and Georgi Kantchev. “Satellite Images Show Russia’s Expanding Ukraine Buildup.” *Washington Post*, 20 April 2021: https://www.wsj.com/articles/satellite-images-show-russias-expanding-ukraine-buildup-11618917238.

Grisé, Michelle, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska. “*Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation*.” RAND Corporation, Washington, 18 August 2022: https://www.rand.org/pubs/research_-reports/RRA198-8.html.

Guerrero-Saade, Juan Andres. “HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine.” *SentinelLabs*, February 28, 2022: https://-www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/.

Guerrero-Saade, Juan Andres and Max van Amerongen. “AcidRain | A Modem Wiper Rains Down on Europe.” *SentinelLabs*, March 31, 2022: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

Hammond-Errey, Miah. “Elon Musk’s Twitter Is Becoming a Sewer of Disinformation.” *Foreign Relations*, July 15, 2023: https://foreignpolicy.-com/2023/07/15/elon-musk-twitter-blue-checks-verification-disinformation-propaganda-russia-china-trust-safety/.

Harknett, Richard J and Max Smeets. “Cyber Campaigns and Strategic Outcomes.” *Journal of Strategic Studies* 45, no. 4 (2022): 534–67

Harris, Shane and Paul Stone. “Russia Planning Massive Military Offensive Against Ukraine Involving 175,000 Troops, US Intelligence Warns,” *Washington Post*, December 2, 2021: https://www.washingtonpost.com/-national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

Harrison Dinnis, Heather. *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, 2012.

Healey, John. “Preparing for Inevitable Cyber Surprise.” *War on the Rocks*, January 12, 2022: https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/.

Hegel, Tom and Aleksandar Milenkoski. “NoName057(16) – The Pro-Russian Hacktivist Group Targeting NATO,” *SentinelLabs*, January 12, 2023: https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/.

Heijmans, Philip. “Ukraine Sees Russian Cyberattacks Growing More Sophisticated.” *Bloomberg*, 24 October 2023: https://www.bloomberg.com/-news/articles/2023-10-24/ukraine-sees-russian-cyberattacks-growing-more-sophisticated?embedded-checkout=true.

Hoffman, Frank G. “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War.” In *2016 Index of US Military Strength: Assessing America’s Ability to Provide for the Common Defence*, edited by Dakota L Wood, 25–36. Washington: The Heritage Foundation, 2016.

Hollis, David. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal* (2011): 1–10: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Holmes, David. “Virtual Politics – Identity and Community in Cyberspace.” In *Virtual Politics: Identity and Community in Cyberspace*, edited by David Holmes, 1-24. London, Thousand Oaks, and New Delhi: Sage Publications, 1997.

Ignatius, David. “Russia’s Radical Strategy for Information Warfare.” *Washington Post*, January 18, 2017: https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/.

InMind. *Ukrainian Media Use and Trust in 2022*. USAID and Internews, 2022: https://internews.in.ua/wp-content/uploads/2022/11/USAID-Internews_Media-Consumption-Survey_2022_eng-1.pdf; Willet, "The Cyber Dimension."

Jasper, Scott. *Russian Cyber Operations: Cording the Boundaries of Conflict*. Washington: Georgetown University Press, 2022.

Jonsson, Oscar. *The Russian Understanding of War: Blurring the Lines Between War and Peace*. Washington: Georgetown University Press, 2019.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven and London: Yale University Press, 2018.

Kello, Lucas. "Cyber Legalism: Why It Fails and What to Do about It." *Journal of Cybersecurity* 7, no. 1 (2021): 1-15.

Kello, Lukas *Striking Back: The End of Peace in Cyberspace – And How to Restore It*. New Heaven and London: Yale University Press, 2022.

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

Ksenia Ilyuk, Yevhen Sapolovich, and Ira Ryaboshtan. "'Now We Will Live to the Fullest!' How and Why Russia Has Created a Telegram Channels Network for the Occupied Territories of Ukraine." Detector Media, May 5, 2022: https://detector.media/monitorynh-internetu/article/199010/2022-05-05-now-we-will-live-to-the-fullest-how-and-why-russia-has-created-a-telegram-channels-network-for-the-occupied-territories-of-ukraine/.

Komarov, Dmitriy. "Рік - Частина четверта [Year – Part Four]." *Світ навиворіт* [The World Inside Out], May 19, 2023: https://www.youtube.com/watch?v=yaOE1SDvJ6A.

Kononov, Nickolay. "The Kremlin's Social Media Takeover." *The New York Times*, 10 March, 2014: https://www.nytimes.com/2014/03/11/opinion/the-kremlins-social-media-takeover.html.

Kostyuk, Nadiya and Erik Gartzke. "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine." *Texas National Security Review* 5, no. 3 (2022): 113–26.

Kostyuk, Nadiya and Erik Gartzke. "Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations." *Journal of Conflict Resolution*, online first (2023): 1-28.

Laje, Diego. "Ukraine's Fusion of Cyber and Kinetic Warfare: Illia Vitiuk's Stand Against Russian Cyber Operations." *Signal (AFCEA International)*,

September 15, 2023: https://www.afcea.org/signal-media/test-signal-landing-page-format/ukraines-fusion-cyber-and-kinetic-warfare-illia.

Lawson, Sean T *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. London and New York: Routledge, 2020.

Lehto, Martti. "Cyber Warfare and War in Ukraine." *Journal of Information Warfare* 2, no. 1 (2023): 61–75.

Lemay, Antoine. "Survey of Publicly Available Reports on Advanced Persistent Threat Actors." *Computers & Security* 72 (2018): 26-59.

Libicki, Martin. "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8, no 2 (2012): 321-36.

Libicki, Martin. *Cyberspace in Peace and War*. Annapolis: Naval Institute Press: 2021.

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no 3 (2012): 401–28.

Lilly, Bilyana. *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*. Annapolis: Naval Institute Press, 2022.

Lin, Herbert. "The Existential Threat from Cyber-Enabled Information Warfare." *Bulletin of the Atomic Scientists* 75, no 4 (2019): 187–96.

Lin, Herbert. "Russian Cyber Operations in the Invasion of Ukraine." *The Cyber Defence Review* 7, no 4 (2022): 31–45.

Macias, Amanda and Michael Scheetz. "Pentagon awards SpaceX with Ukraine contract for Starlink satellite internet." *CNBC*, 1 June 2023: https://www.cnbc.com/2023/06/01/pentagon-awards-spacex-with-ukraine-contract-for-starlink-satellite-internet.html.

Maschmeyer, Lennart, Ronald J. Deibert, and Jon R. Lindsay. "A Tale of Two Cybers - How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society." *Journal of Information Technology & Politics* 18, no 1 (2021): 1–20.

Maschmeyer, Lennart. "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." International Security 46, no 2 (2021): 51–90, p 55.

Maschmeyer, Lennart and Nadiya Kostyuk. "There is no Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict." War on the Rocks, 8 February 2022: https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

Maschmeyer, Lennart and Myriam Dunn Cavelty. "Goodbye Cyberwar: Ukraine as Reality Check." *Policy Perspectives* 10, no 3, CSS ETH Zürich, 2023:

https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf.

Matishak, Martin. “Russia Could Launch Digital Offensive against Ukraine, Administration Official Warns.” *The Record: Recorded Future News*, 6 December 2021: https://therecord.media/russia-could-launch-digital-offensive-against-ukraine-administration-official-warns.

Matthews, Owen. *Overreach: The Inside Story of Putin’s War Against Ukraine*. London: Mudlark, 2022.

McGuffin, Chris and Paul Mitchell. “On Domains: Cyber and the Practice of Warfare.” *International Journal: Canada’s Journal of Global Policy Analysis* 69, no 3 (2014): 394-412.

McLaughlin, Jenna. “Russia Bombards Ukraine with Cyberattacks, but the Impact Appears Limited.” *NPR*, 3 March 2023: https://www.npr.org/-2023/02/23/1159039051/russia-bombards-ukraine-with-cyberattacks-but-the-impact-appears-limited.

Meurant, Sébastien and Rémi Cardon. *Rapport d’information fait au nom de la délégation aux entreprises relatif à la cybersécurité des entreprises*. Report no 678, The French Senat, 10 June 2021: https://www.senat.fr/rap/r20-678/r20-6781.pdf.

Merrian-Webster. “Cyber.” 27 August 2023: https://www.merriam-webster.com/dictionary/cyber.

Miller, Maggie. “Russian Invasion of Ukraine Could Redefine Cyber Warfare.” *Politico*, 28 January 2022: https://www. politico.com/news/-2022/01/28/russia-cyber-army-ukraine-00003051.

Miller, Maggie. “The World Holds Its Breath for Putin’s Cyberwar.” *Politico*, 23 March 2022: https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440.

Mitchell, Russ. “How Amazon Put Ukraine’s ‘Government in a Box’ - And Saved Its Economy from Russia.” *Los Angeles Times*, December 15, 2022: https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data.

Monte, Matthew. *Network Attacks and Exploitation: A Framework*. Wiley: Indianapolis, 2015.

Moore, Daniel. *Offensive Cyber Operations: Understanding Intangible Warfare*. London, Hurst & Company, 2022.

Moynihan, Harriet. “The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace.” *Journal of Cyber Policy* 6, no. 3 (2021): 394–410.

Pearce, James C. “Hybrid” and “Information”: New Labels, Old Politics.” In *Hybrid Conflicts and Information Warfare: New Labels, Old Politics*, edited by Ofer Fridman, Vitaly Kabernik, and James C Pearce, 1-8. Lynne Rienner Publishers: Boulder and London, 2019.

Plokhy, Serhii. *The Russo-Ukrainian War*. Dublin: Allen Lane, 2023.

Polyakova, Alina. “Want to know what’s next in Russian election interference?” *Brookings Institute*, March 28, 2019: https://www.brookings.edu/-articles/want-to-know-whats-next-in-russian-election-interference-pay-attention-to-ukraines-elections/.

Putin, Vladimir. “On the Historical Unity of Russians and Ukrainians.” *President of Russia*, July 12, 2021: http://en.kremlin.ru/-events/president/news/66181.

Qrator Labs. “The National Internet Segment Reliability Research.” *Medium*, 8 September, 2022: https://qratorlabs.medium.com/the-2022-national-internet-segment-reliability-research-60bd1278759b.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

Sabbagh, Dan. “Fury in Ukraine as Elon Musk’s SpaceX Limits Starlink Use for Drones.” *The Guardian*, February 9, 2023: https://www.theguardian.com/world/2023/feb/09/zelenskiy-aide-takes-aim-at-curbs-on-ukraine-use-of-starlink-to-pilot-drones-elon-musk.

Sambaluk, Nicholas Michael. *Myths and Realities of Cyber Warfare: Conflict in the Digital Realm*. Santa Barbara: Praeger Security, 2020.

Satter, Raphael. “Satellite Outage Caused ‘Huge Loss in Communications’ at War’s Outset – Ukrainian Official.” *Reuters*, 15 March 2022: https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/.

Shandler, Ryan Michael L. Gross, and Daphna Canetti. “Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis.” *Journal of Global Security Studies* 8, no 1 (2022): 1–19.

Sharp, Travis. “Hiding in Plain Sight: Political Effects of Cyber Operations.” *Survival 60*, no. 6 (2018): 45–53, p 48.

Schectman, Joel, Christopher Bing, and James Pearson. “Ukrainian Cyber Resistance Group Targets Russian Power Grid, Railways.” *Reuters*, 1 March 2022: https://www.reuters.com/technology/ukrainian-cyber-resistance-group-targets-russian-power-grid-railways-2022-03-01/; Joe Tidy, “Meet the hacker armies on Ukraine’s cyber front line,” *BBC*, April 15, 2023: https://www.bbc.com/news/technology-65250356.

Shypovskyi, Volodymyr. “Cyber Domain in Russian-Ukrainian War 2022.” Presentation, *Defending Ukraine: The Changing Face of Cyberwarfare*, Swedish Defence University, Stockholm, August 23, 2023 [referenced with the approval of author].

Smalley, Suzanne. “Cybersecurity experts question Microsoft’s Ukraine report.” *Cyberscoop*, July 1, 2022: https://cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/.

Smeets, Max. “The Strategic Promise of Offensive Cyber Operations.” *Strategic Studies Quarterly* 12, no. 3 (2018): 90–113.

Smeets, Max. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Hurst: London, 2022.

Soldatov, Andrei and Irina Borogan. “Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities.” CEPA, 2022: https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

Sonne, Paul, 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/.

Spînu, Natalia. *Ukraine Cybersecurity: Governance Assessment*. Geneva Centre for Security Sector Governance (DCAF), 2020: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

Stapley, Emily, Sally O’Keeffe, and Nick Midgley. “Developing Typologies in Qualitative Research: The Use of Ideal-Type Analysis.” *International Journal of Qualitative Methods* 21, online first (2022): 1-9

Štrucl, Damjan. “Russian Agression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare.” *Contemporary Military Challenges* 24, no. 2 (2022): 103–123.

Strömblad, Christoffer. “State-Sponsored Cyber Attacks Against Ukraine.” *Trusec*, January 19, 2022: https://www.truesec.com/hub/blog/state-sponsored-cyber-attacks-against-ukraine.

Swisher, Kara. “Are We Ready for Putin’s Cyber War? I Asked One of Biden’s Top Cybersecurity Officials.” Sway (podcast), *The New York Times*, March 10, 2022: https://www.nytimes.com/2022/03/10/opinion/sway-kara-swisher-anne-neuberger.html?showTranscript=1.

Tkachenko, Oleksii. “Cybersecurity in Ukraine: National Strategy and International Cooperation.” GFCE, June 7, 2017:

https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/.

Valeriano, Brandon and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford and New York: Oxford University Press, 2015.

van Sant, Shannon and Clothilde Goujard. "European Parliament Website Hit by Cyberattack after Russian Terrorism Vote." *Politico*, November 23, 2022: https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/.

Vendil Pallin, Carolina. *Nyckelaktörerna för rysk cyberstrategi: 2000–2020*. FOI-R--5025--SE, Totalförsvarets forskningsinstitut, Stockholm, 2020: https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5025--SE.

Vendil Pallin, Carolina. *Moscow's Digital Offensive: Building Sovereignty in Cyberspace*. FOI Memo 7521, Swedish Defence Research Agency, Stockholm, 2021: https://www.foi.se/rapporter/-rapportsammanfattning.html?reportNo=FOI%20Memo%207521.

Vendil Pallin, Carolina, Maria Engqvist and Carl Michael Gräns. "Russia's National Security: Fighting the West for Regional Hegemony." In *Russia's War Against Ukraine and the West: The First Year*, edited by Maria Engqvist and Emil Wannheden, FOI-R--5479—SE, Swedish Defence Research Agency, Stockholm, 2023, 33-44: https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5479--SE.

Voo, Julia. "Lessons from Ukraine's Cyber Defense and Implications for Future Conflict." In *Evolving Cyber Operations and Capabilities*, edited by James A Lewis and Georgia Wood, Center for Strategic & International Studies, Washington, 2023, 15-22: https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities.

Waqas. "List of Proxy IPs Exposed to Block Killnet's DDoS Bots." *HackRead*, February 8, 2023: https://www.hackread.com/killnets-proxy-ips-blocks-ddos-bots/.

Whyte, Christopher and Brian Mazanec. *Understanding Cyber-Warfare: Politics, Policy, and Strategy*. London and New York: Routledge, 2021.

Wilde, Gavin. "Cyber Operations in Ukraine: Russia's Unmet Expectations." Working Paper, Carnegie Endowment for International Peace, Washington, 2022: https://carnegieendowment.org/files/202212-Wilde_RussiaHypotheses-v2.pdf.

Willett, Marcus. “The Cyber Dimension of the Russia–Ukraine War.” *Survival* 64, no. 5 (2022): 7–26.

Zabrodskyi, Mykhaylo, Jack Watling, Oleksandr Danylyuk V, and Nick Reynolds. *Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine: February–July 2022*. Royal United Services Institute for Defence and Security Studies (RUSI), London, 2022: https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

Zetter, Kim. “Viasat Hack ‘Did Not’ Have Huge Impact on Ukrainian Military Communications, Official Says.” *Zero Days*, September 26, 2022: https://www.zetter-zeroday.com/p/viasat-hack-did-not-have-huge-impact.

ISSN 1650-1942

www.foi.se