Sotnyk Artem,
master student,
Simon Kuznets Kharkiv National University of Economics, Kharkiv

CYBER SECURITY IMPORTANCE DURING THE RUSSIAN-UKRAINIAN WAR

Abstract. The Russian–Ukrainian war demonstrates that modern armed conflicts extend far beyond traditional physical domains into cyberspace, where states seek strategic advantages through disruption, espionage, and information operations. This article examines the evolution, objectives, and effectiveness of Russian cyber operations against Ukraine, placing them within a broader historical and strategic context. Drawing on documented cyber incidents (from early attacks in Estonia and Georgia to large-scale operations such as BlackEnergy, NotPetya, and cyber-enabled influence campaigns) the study highlights how cyber tools have been integrated into Russia's broader military and political strategy. Particular attention is paid to the full-scale invasion of Ukraine, during which cyberattacks have increasingly targeted civilian infrastructure in an attempt to undermine morale and societal resilience. Despite persistent threats, Ukraine has demonstrated remarkable adaptability, supported by strong public–private partnerships, international cooperation, and pre-war investments in cybersecurity. The article argues that while cyber operations can shape the strategic environment, their direct military impact remains limited and often unpredictable. Ultimately, the Ukrainian case offers important lessons for enhancing cyber resilience, strengthening international cooperation, and rethinking approaches to counter cyber-enabled information warfare in future conflicts.

Keywords: cybersecurity; cyber warfare; Russian–Ukrainian war; critical infrastructure; information operations; cyber resilience; public–private partnerships.

Анотація. Російсько-українська війна демонструє, що сучасні збройні конфлікти виходять далеко за межі традиційних фізичних сфер і йдуть у кіберпростір, де держави прагнуть стратегічних переваг шляхом деструктивної діяльності, шпигунства та інформаційних операцій. У цій статті розглядається еволюція, цілі та ефективність російських кібероперацій проти України, розміщуючи їх у ширшому історичному та стратегічному контексті. Спираючись на задокументовані кіберінциденти — від ранніх атак в Естонії та Грузії до масштабних операцій, таких як BlackEnergy, NotPetya та кіберкампаній впливу — дослідження висвітлює, як кіберінструменти були інтегровані в ширшу військову та політичну стратегію Росії. Особлива увага приділяється повномасштабному вторгненню в Україну, під час якого кібератаки все частіше були спрямовані на цивільну інфраструктуру, намагаючись підірвати моральний дух та стійкість суспільства. Незважаючи на постійні загрози, Україна продемонструвала надзвичайну адаптивність, що підтримується міцними державно-приватними партнерствами, міжнародною співпрацею та довоєнними інвестиціями в кібербезпеку. У статті стверджується, що хоча кібероперації можуть формувати стратегічне середовище, їхній прямий військовий вплив залишається обмеженим і часто непередбачуваним. Зрештою, український випадок пропонує важливі уроки для підвищення кіберстійкості, зміцнення міжнародної співпраці та переосмислення підходів до протидії інформаційній війні, що ведеться в кіберпросторі, у майбутніх конфліктах.

Ключові слова: кібербезпека; кібервійна; російсько-українська війна; критична інфраструктура; інформаційні операції; кіберстійкість; державно-приватне партнерство.

Introduction. In the third year of the Russian full-scale invasion of Ukraine, it has become evident that modern military conflicts are no longer confined to traditional domains such as land, sea, and air, but are increasingly fought within the domain of cyberspace. Cyber operations now play a critical role in shaping the strategic environment, complementing conventional military actions through espionage, disruption of critical infrastructure, and information warfare. The Russian–Ukrainian war provides a clear example of how cyber capabilities are employed alongside

kinetic operations to influence political decision-making, undermine public trust, and weaken an adversary's resilience. As digital technologies become deeply embedded in state governance, military systems, and civilian life, cybersecurity has emerged as a crucial element of national defense. The purpose of this article is to analyze the significance of cybersecurity during the Russian–Ukrainian war by examining key cyberattacks, identifying major threats, and assessing their broader implications for contemporary and future armed conflicts.

Goal. The purpose of this article is to summarize the major cyber attacks and threads and the overall importance of cyber security during the Russian-Ukrainian war.

Main material. Examining the history of Russian cyber operations reveals that the Kremlin utilizes cyber capabilities to engage in long-term competition with its rivals. Prior to 2014, Moscow's campaigns primarily focused on political warfare and espionage, with notable operations in Estonia and Georgia. In 2007, large-scale denial-of-service attacks targeted Estonia after the country relocated the Bronze Soldier monument, punishing it for this action. During the Russo-Georgian conflict in 2008, Russia employed cyberattacks to support information operations (IO) designed to manipulate, disrupt, corrupt, or usurp the decision-making processes of adversaries while safeguarding its own interests [1; 2; 3].

In a precursor to its military campaign aimed at destroying Ukrainian critical infrastructure, Moscow targeted Kyiv's power supply using cyber operations. After the illegal annexation of Crimea in 2014, advanced persistent threat (APT) groups, including Sandworm, were involved in the 2015 BlackEnergy campaign, which targeted Ukrainian power generation and distribution systems. While these attacks received significant media attention, they had limited operational impacts. In 2017, Russian-affiliated groups launched the NotPetya campaign, which inadvertently affected global logistics beyond its intended targets in Ukraine [4; 5].

Russia has also employed cyber operations as a form of political warfare, utilizing a blend of propaganda to polarize societies and influence political elections. Notably, these efforts included disruption campaigns that sought to deface websites and depict supporters of Ukraine as Nazis [1]. This was followed by a more brazen attempt to undermine confidence in U.S. democracy through cyber operations during the 2016 presidential election, the effects of which are still debated. In 2018, U.S. Cyber Command launched a preemptive operation against the Internet Research Agency – a Russian firm focused on propaganda and influence—based on historical behavior and clear indicators that Moscow was preparing to repeat its interference in the upcoming midterm elections.

More recently, Russian operations have blended sophisticated espionage with criminal malware campaigns. Throughout 2020, the Russian hacking group APT29, also known as Cozy Bear, exploited a supply chain vulnerability within the SolarWinds Orion program to steal data and digital tools from a wide range of targets. This operation raised alarm bells because neither the NSA nor major firms like Microsoft detected the intrusion, which likely involved a combination of human intelligence and cyber operations to implant malicious code deep within the servers. In 2021, criminal actors identified as DarkSide, likely linked to the Russian state, successfully deployed ransomware against Colonial Pipeline, a critical system that supplies much of the fuel used on the U.S. East Coast.

During the full-scale invasion, most of Russia's cyberattacks appear to be aimed at disrupting daily life. For example, they often target the electricity supply or create unstable internet connections. The hackers' objective seems to be to make life so uncomfortable that Ukrainians lose hope in themselves and their leaders and ultimately abandon the fight for their independence and territory. As strange as it may sound, Moscow has made the demoralization of civilians in cyberspace a key strategy in its approach to warfare [5; 6; 7].

However, Ukrainians have shown remarkable resilience, consistently bouncing back from each cyber disruption. They have even gained support from some of the world's largest technology companies to ensure their infrastructure is more secure than ever. Ukraine has also emerged as one of the most digitally connected and technologically advanced countries in Europe. While it is essential to acknowledge the suffering and costs imposed by Russian cyberattacks, Ukraine's adaptability is crucial in any analysis of the role of cyber operations in armed conflict.

In Russia's case, hackers are incentivized to be as disruptive and opportunistic as possible – especially considering that the alternative is being sent to the front lines with a rifle. The threats Russia poses to stability in cyberspace are very real; however, these disruptions may ultimately work against the Kremlin in its efforts to win both Ukrainian territory and the support of its people. While Russian hackers may demand significant attention, it is important to ask what they are actually achieving and what lessons could be learned from the Ukrainian resilience in order to protect critical cyber infrastructure from future attacks and threats.

The case of Ukrainian cyber defense suggests expanding public-private partnerships and improving collective defense mechanisms in cyberspace to counter cyber threats. There are three key recommendations for enhancing cyber defense [8; 9; 10].

Firstly, increasing public-private partnerships is crucial. Securing critical intelligence and military networks is not enough; modern societies rely on interconnected public and private networks to the higher extend. Encouraging collaboration through pooled data and common standards can thwart adversaries. Government incentives, such as tax credits for companies aiding crisis efforts, could strengthen cyber defenses. Also, leveraging transparent pooled data on cyber threats is crucial. While progress has been made, the countries governments should create a continuously updated, anonymized data pool, drawing parallels with economic data practices. This would enable both sectors to identify attack trends and adapt defenses accordingly. Overall, pooled data acts as a public good, enhancing collaboration and allowing for targeted cyber operations against emerging threats.

The second recommendation is to enhance diplomatic engagement in cyber defense and intelligence sharing. The government should coordinate with partners and allies to secure cyberspace. While this is straightforward to propose, implementing it requires collaboration across various agencies.

Ukraine's resilient networks have benefited from pre-conflict actions to develop a national cyber strategy, illustrating the importance of both the private sector and foreign governments in helping Kyiv prepare for increased cyber threats.

Two key areas for diplomatic outreach in cybersecurity are information sharing and interoperability. Firstly, the government must accelerate the sharing of knowledge of vulnerabilities with partners. Currently, many governments withhold information to protect sources or because vulnerabilities relate to active exploits. This creates bureaucratic barriers that hinder timely sharing and foster distrust among partners.

Secondly, diplomatic outreach should build interoperability with allies by increasing crisis simulations and cyber exercises to cultivate a common understanding of coordinated responses. Such activities could simulate simultaneous critical infrastructure attacks across nations, preparing partners for potential global threats from rogue states like Russia or China.

The third recommendation is to reevaluate strategies for countering cyber-enabled information operations. Insights from the initial year of the conflict in Ukraine indicate that defending against misinformation is more challenging than combating malware. Consequently, governments need to create a credible and adaptive approach to respond to cyber-enabled information operations and computational propaganda. The obstacles associated with countering global propaganda are significant, making it unlikely that any single agency or method can effectively tackle them. Thus, for instance, the U.S. Congress should establish a new commission tasked with examining the most effective ways to address misinformation as it pertains to the broader U.S. national security strategy and the limitations of current legal authorities. Previous commissions, such as the U.S. Cyberspace Solarium Commission, demonstrate how to drive change regarding the protection of cyberspace and can serve as a reference point.

Conclusion. Summing up, the integration of cyberspace in military operations is now essential, evolving faster than the historical shift to written military orders. Current warfare trends challenge the effectiveness of the term "cyberwar," suggesting that cyber operations are often more suited for espionage and strategic shaping rather than direct tactical advantages. The conflict in

Ukraine highlights the importance of analyzing cyber power, particularly from states like Russia, as future wars will likely rely on cyberspace.

Although cyber operations can support military efforts, their impact is indirect, often limited by the need for intelligence assessments and the risks associated with operational access. Commanders must balance the desire to use cyber capabilities with the fear of future losses, resulting in a preference for more tangible options like artillery.

Moreover, while Moscow may reserve significant cyber resources as a deterrent, past attempts to disrupt critical infrastructure have shown limited success. The effectiveness of cyber-enabled political warfare also remains uncertain, as public resilience to misinformation is unpredictable – citizens may either adapt or become more cynical and mistrustful amidst the deluge of misinformation that accompanies warfare.

References

1. Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures. *Center for Strategic and International Studies*. URL: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.
2. Maschmeyer L. Cyber Conflict and Subversion in the Russia-Ukraine War. *Lawfare: website*. URL: https://www.lawfaremedia.org/article/cyber-conflict-in-the-russia-ukraine-war
3. Bosch O. Critical Information Infrastructure and Cyber-Terrorism. *Law, Policy, and Technology*. P. 31–40. URL: https://doi.org/10.4018/978-1-61520-831-9.ch003
4. Duguin S. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. Directorate-general for external policies of European Parliament: policy department. Workshop. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.
5. Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine. *Canadian Center for Cyber Security*. URL: https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf
6. Cyber considerations from the conflict in Ukraine. *KMPG: website*. URL: https://kpmg.com/dk/en/home/insights/2022/03/cyber-considerations-from-the-conflict-in-ukraine.html
7. Wilde G. Why Cyber Attacks on Ukrainians Aren't Working the Way Russia Expected. *Emissary: website*. URL: https://carnegieendowment.org/emissary/2024/03/why-cyber-attacks-on-ukrainians-arent-working-the-way-russia-expected?lang=en.
8. Onyshko D. Cyber Security: Learn the Basics of Cyber Security, Threat Management, Cyber Warfare Concepts and Executive-Level Policies. Independently Published, 2020.
9. Poitevin V. Use of cyber-tools in the Russian-Ukrainian war: a strategic analysis of a major first. *Stormshield: website*. URL: https://www.stormshield.com/news/cyber-warfare-use-of-cyber-tools-in-the-russian-ukrainian-war.
10. Slonopas A. What is Cyber Warfare? Various Strategies for Preventing It. *American Public University*. URL: https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare.