International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 07 Issue 11 November 2024

DOI: 10.47191/ijsshr/v7-i11-37**,** Impact factor- 7.876

Page No: 8466-8472

Ukraine's Strategy to Counter Russian Cyber Threats in the Russo–Ukrainian War

Billy Jeremie Sarimin[1], Angel Damayanti[2]

[1,2]Universitas Kristen Indonesia

ABSTRACT: This study investigates the cyber threats that Russia poses to Ukraine and examines the strategies that Ukraine employs in response. The Russian cyber operations are believed to have started covertly before the beginning of the Russia-Ukraine War in 2022. These operations peaked when Russia targeted the Kyiv Post news agency and the KA-SAT satellite, resulting in significant communication disruptions and power outages within Ukraine, which affected both the government and society. The research utilizes theories of security strategy, cyber threats, and cybersecurity strategy to analyze the cyber tactics used during the Russia-Ukraine conflict. Employing qualitative methods and case study models, the study describes Russia's cyber operations that threaten Ukraine's security, as well as Ukraine's responses to these threats. The operations included information manipulation and attacks on critical infrastructure. Findings reveal that the Ukrainian government implemented several effective strategies, such as establishing legal frameworks, creating cybersecurity agencies, and collaborating with the United States. These measures have proven successful in countering Russian cyber-attacks. Through its partnership with the U.S., Ukraine's rapid response team (CERT) was able to recover systems that had been targeted, thereby enhancing Ukraine's cyber resilience against Russian threats.

KEYWORDS: cyber threats, Russia-Ukraine conflict, cybersecurity strategy

BACKGROUND

The Russia-Ukraine conflict is not only military in nature but also extends into cyberspace, with Russia using its cyber capabilities to threaten and attack Ukraine. Prior to the military invasion in 2022, Russia had already launched several cyberattacks against Ukraine. These included attempts to sabotage the results of Ukraine's presidential election in 2014, a power outage that affected western Ukraine for several hours in 2015, and a significant attack in 2022 on the Kyiv Post news agency and the KA-SAT satellite. Russia's assault on Ukrainian news agencies has been notably effective; it has disrupted communication systems and networks, making it difficult for Ukrainians to access information and obtain official statements from their government. (Samad and Persadha, 2022: 140)

Russia has been accused of conducting cyber operations against various countries to obtain confidential information essential for developing strategies that advance its national interests. One such target is Germany. A report from 2017 indicated that Russia successfully hacked the cyber systems of the German Ministry of Foreign Affairs and the Ministry of Defense (Limnell 2018, 69). Additionally, there are rumours that Russia aims to hack the systems of several other EU member states to access similar information (Limnell, 2018: 71). Russia is known to often carry out cyber-attacks in the form of Distributed Denial of Service (DDoS) attacks and website defacements, temporarily rendering websites inaccessible (European Parliamentary Research Service, 2022).

The development of cyber capabilities in Russia began when several military officials recognised that such weapons could undermine other countries and pose a significant threat (Jaitner, 2015: 87). Russia understands that combining technology, military operations, strategy, and political decisions is essential to achieving its national interests (Wirtz, 2015: 30). Based on these insights, Russia began integrating space and cyber operations into its primary national defence and security strategy. In response to the realisation that cyber operations can jeopardise a nation's security, several countries established agencies dedicated to addressing threats from foreign cyber capabilities. For instance, Israel has Unit 8200 under the Israel Defence Forces, the United States has the United States Cyber Command, and Australia operates the Cyber Security Operational Centre. (Babys, 2021: 426).

Recognising the critical importance of cybersecurity for a country, this article specifically addresses the formulation of Ukraine's strategy in responding to Russian threats and cyberattacks, particularly in the context of the ongoing Russia-Ukraine conflict. This research is organised into three sections: introduction, findings, discussion, and conclusion. The findings section discusses the use of cyber as a threat, Russian cyber developments, and how Russia employs its cyber capabilities in the Russia-Ukraine conflict. This section will also explain how the Ukrainian government has overcome Russian cyber threats.

The authors use a qualitative methodology to examine how the Ukrainian government responded to Russia's cyber-attacks during the Russo-Ukrainian conflict. A case study approach is employed to provide a detailed overview of the cyber threats posed by Russia to Ukraine's security and to explain the strategies Ukraine used to counter these threats. This research incorporates qualitative data from various sources, including books, journals, legal documents, research reports, government publications, and print and online news media. The data is categorised and analysed from multiple perspectives to ensure a comprehensive and objective assessment.

THEORETICAL FRAMEWORK

This research focuses on three key concepts in international security: security strategy, cyber threats, and cybersecurity strategy. A security strategy involves a country's efforts to maintain security and enhance its capabilities using economic, political, social, and military power (Yarger, 2006, 1). This strategy aims to achieve national interests. However, as noted by David Alberts in Groh (2008, 324), technological advances in the global community have necessitated changes in military strategies to address new threats. It is essential to incorporate technology, especially information and communication technology, into a military strategy to effectively tackle the cyber threats that have emerged over the past three decades. Given this framework, it is evident that countries, including Ukraine, require an appropriate strategy to counter the cyber threats posed by Russia, particularly in the context of the ongoing Russia-Ukraine conflict.

The threat of cybercrime, including account hacking, fraud, and the theft of personal and confidential data, has made cybersecurity a significant concern for governments. According to
Rid and McBurney (2017, 7), cyber threats originate from lines of computer program code. This code can disrupt social activities and cause both physical and system damage. Cyberspace refers to a realm where individuals communicate through the internet, enabling cross-border connections and information exchange (Harianja, Arionto, and Setiawan, 2022: 94). Additionally, Phillip Mirowski noted that "cyborg science reflects the new interaction between humans and machines. This interaction blurs the distinction between nature and society, as one model begins to resemble the other and between 'reality' and 'simulacra'" (Lawrence, 2013:
148).

In the context of the Russia-Ukraine conflict, cyberattacks on Ukraine have led to significant communication disruptions and power outages, impacting the daily operations of both the government and society. Philip Mirowski argues that addressing cyber threats requires a combination of human and technological roles (Lawrence, 2013: 148). This situation highlights a shift in how a country's strength is perceived; conventional military forces alone are no longer sufficient. Instead, combining human expertise and advanced technology is essential for effectively tackling cyber threats. Consequently, it can be concluded that cyber threats arise from the interaction of human actions and technology, specifically through the use of computers and the creation of software code. Therefore, overcoming these challenges necessitates an integrated approach that combines human capabilities with technological advancements.

A country's ability to establish cybersecurity combines policies, tools, actions, technologies, and training to safeguard governmental, individual, and private sector data in cyberspace (International Telecommunication Union, 2018: 13). Therefore, conducting system analysis and risk management is essential. This article will explore how a country, particularly
Ukraine, progresses from the initial stages to international cooperation in addressing cyber threats directed at it. The initial stage involves the formation of a legal framework for the stakeholders engaged in cybersecurity. On the other hand, international cooperation consists of countries collaborating to enhance their cybersecurity efforts (International
Telecommunication Union, 2018: 18-48).

FINDINGS AND DISCUSSION

The Use of Cyber as a Threat

Cyber capabilities can be profitable and threatening for a government, especially as information and communication technology advances and public reliance on these technologies increases. In the realm of international relations and conflict, the cyber domain has become a battleground for power competition, serving as a vital space for storing and disseminating data, including sensitive information held by national governments. Research by Febrianti, Hara, and Sunarko (2022) supports this notion by discussing the Indian government's initiative to ban several Chinese-made applications that have gained popularity in cyberspace. The Indian government implemented this ban due to concerns over data storage and control practices associated with these applications, protected under China's National Intelligence Law.

The potential for non-traditional actors to use cyber capabilities for profit by threatening cyber-attacks is significant. These actors can include individuals commonly called hackers or professional groups organised by an agency. A notable example of this occurred when Edward Snowden, a former contractor for the National Security Agency (NSA) in the United States, leaked information about cyber operations directed at Indonesia. These operations involved intercepting personal communications of President Susilo Bambang Yudhoyono and several other Indonesian officials at the time. This incident prompted the Indonesian

government to establish the Cyber Defense Center, operating under the Ministry of Defense, and the State Cyber and Cryptography Agency (BSSN). They aim to monitor cyberspace for foreign intelligence activities and to identify individuals attempting to conduct hacking activities (Krisnata, Reksoprodjo, and Waluyo, 2022).

Cyber threats and attacks are not limited to a single country; they can affect multiple nations within a region. Novitasari (2017) highlighted in her research that the high level of internet access in Southeast Asia is not matched by adequate cybersecurity measures, making the region particularly vulnerable to cyber-attacks. Her research indicates that the cyber realm has evolved into a military domain that poses severe risks to national security through activities such as eavesdropping, espionage, and sabotage. Consequently, as a regional organisation, ASEAN is committed to developing information infrastructure, aiming to enhance cybersecurity in the Southeast Asia.

The significance of cyberspace has grown considerably, particularly for countries with contentious relationships. This shift indicates that the conflict landscape has expanded from physical confrontations to the digital realm. Pratiwi (2019) highlights this dynamic in the context of India-Pakistan relations, where both nations frequently launch cyberattacks against each other. For instance, Pakistan has conducted cyber operations aimed at leaking sensitive information from India. This data is then disseminated to the media and within Pakistan's government for political purposes. In response, the Indian government established the National Critical Information Infrastructure Protection Centre, tasked with overseeing crucial information systems in sectors such as energy, communications, and air traffic management.

In his article "The Cyber Dimension of the Russia-Ukraine War," Marcus Willet (2022) explains that Russia has allegedly utilized its cyber forces since the conflict with Georgia in mid-2008. His research highlights how Russia carried out cyberattacks through the Distributed Denial of Service (DDoS) program, targeting the official website of the Georgian government. As a result, several government websites became temporarily inaccessible to officials and the general public. Additionally, Russia interfered with Georgia's internet network access, complicating communication for the Georgian military.

During the cyberattacks against Georgia, Russia strengthened its internal defenses, mainly focusing on enhancing cybersecurity within its borders. This effort coincided with a disinformation campaign to distribute misinformation to the Georgian populace. The goal was to complicate the Georgian government's efforts to disseminate factual news (Willet 2022, 10). Consequently, this led to a decline in trust among Georgians toward their leaders and created divisions within the country.

Similarly, Russia employed cyber tactics ahead of the 2016 U.S. presidential election. In their article, Basuki Erwin Setiyadi and Makmur Keliat (2020) revealed that Russia allegedly used its cyber capabilities during the political campaign to damage the reputation of one of the presidential candidates. This was achieved by leaking confidential data to the public. Although the U.S. government eventually imposed sanctions on Russia, the use of cyber methods resulted in the widespread dissemination of various confidential information, which became public on online media (Setiyadi and Keliat, 2020: 6).

Russian Cyber Developments

Russia's use of cyber capabilities is heavily influenced by developments within the country and the ideas of General Gerasimov, a prominent Russian military official. In 2013, he asserted that the rules and forms of warfare would change in the 21st century, stating that war no longer needs to be formally declared and can take various forms (Fabian, 2019). This perspective led to the formulation of the Gerasimov Doctrine, which encouraged Russian military leaders to integrate cyber elements into their warfare strategies, particularly for gathering intelligence. As a result, cyber capabilities have become as crucial as political, diplomatic, economic, and other non-military elements of Russia's military strategy, especially in the context of information warfare (Morgus et al., 2019; Dziwisz and Sajduk, 2023: 9).

General Gerasimov's perspective emphasises that incorporating cyber capabilities into military strategy aims to influence global public opinion (Morgus et al., 2019, 18-19). He cited the Arab Spring in 2011 as a model for future warfare, illustrating how the strategic use of information can lead to the downfall of one regime and the rise of another (Lilly and Cheravitch, 2020, 132). The U.S. Government has also confirmed Russia's use of cyber tactics for political and security objectives. Its report noted that Russia has established various sites that disseminate propaganda. Notable examples include the Strategic Culture Foundation, which aims to undermine the West, and New Eastern Look, which spreads disinformation related to issues in the Middle East, Asia, and Africa (U.S. Department of State, 2020: 13).

Russia has a distinct approach to information warfare, primarily involving key actors from its intelligence agencies, including The Main Intelligence Directorate (GRU), The Federal
Security Service (FSB), and The Foreign Intelligence Service (SVR) (Morgus et al., 2019: 20). It is suspected that Russia also employs third parties in its operations, allowing them to deny involvement if they are accused of a particular issue. According to Soldatov and Borogan (2018: 18), these actors—from hacker groups to technology companies—receive directives from the Russian government to execute their operations. They are also skilled at concealing the traces of their activities. This operation mode complicates tracing the connection between those who carry out cyberattacks and the primary actors of Russia's cyber operations.

Integrating cyber operations with military operations signifies a paradigm shift in the Russian government's perception of conflict. The change in Russia's perspective can be illustrated in the table below:

Table 1. Changes in Russia's Approach to Conflict

No.	Old Method	New Methods
1.	War needs prior declaration	War can occur without any declaration
2.	War involves direct gun contact, generally involving the army	Contact is made indirectly through various groups and activities
3.	Military conquest greatly determines the control of a territory	Simultaneously conquering the military and economy with specific attacks, as well as conducting attacks on enemy infrastructure
4.	War involves annexation and weakening the enemy's economy	War uses advanced equipment such as lasers, robots, and special operations
5.	War involves all aspects of the military (army, air force, and navy)	War engages civil society
6.	War has strict hierarchy system	War carries out attacks on public facilities
7.		The state provides troops in cyberspace
8.		The state conducts continuous attacks at sea, air, and land
9.		The state employs indirect methods

Source: Berzins (2014)

The shift in military strategy was notably demonstrated when Russia annexed Crimea in 2014, which is claimed as Ukrainian territory. At that time, the Russian government did not deploy a significant military presence; instead, it intensified cyber operations conducted by the Federal
Security Service (FSB) and the Main Intelligence Directorate (GRU) (Bukkvoll, 2016: 16).
The focus of the Russian cyberattacks was on disrupting the communications network of the
Ukrainian government (Jaitner and Mattsson, 2015: 45).

Russia's Cyber Operations in the Russia-Ukraine Conflict

The shift in Russian military strategy has integrated cyber operations with traditional military actions, justifying Russia's cyber-attacks on Ukraine. Since 2013, there have been indications of an increase in Russian cyber-attacks targeting Ukraine, although the impact has often been limited. For instance, some government websites became inaccessible (Pernik, 2018: 61), and Ukrainian officials received fake messages and calls on their mobile phones, which hindered their ability to coordinate efforts (Bergen & Maurer, 2014). In 2014, Russia was accused of attempting to interfere with Ukraine's presidential election by infiltrating the system of the Ukrainian Central Election Commission. It is suspected that Russia fabricated election results by deleting legitimate data and replacing it with false information, indicating a victory for Dmytro Yarosh (Przetacznik & Tarpova, 2022, 3; Greenberg, 2022).

Cyberattacks persisted until 2015. Records from America's Cyber Defense Agency (2021) confirm that Russia executed a successful blackout of power in western Ukraine. This operation directly impacted approximately 225,000 Ukrainians and required about six hours to restore the compromised system (Khan et al., 2016, 56). This attack showcased Russia's cyber capabilities and posed a significant threat to Ukraine's security. As a result, the Ukrainian populace's confidence in their government significantly eroded (Miller, 2021).

Before the military invasion in 2022, Russia executed a cyberattack against Ukraine, targeting the KA-SAT Satellite—a critical asset for the country's communication and army intelligence (Vasquez and Groll, 2023). This assault severely hampered the Ukrainian government's coordination and communication ability. Victor Zhora, the Deputy Chairman and Chief Digital Transformation Officer at the State Service of Special Communication and Information Protection of Ukraine, asserted that this strategic strike placed Ukraine at a significant disadvantage (Bateman 2022, 6). The absence of a robust communication and coordination system during the conflict clearly favours the Russian side.

During the Russia-Ukraine conflict, Russia reportedly focused its cyberattacks on Ukraine's critical infrastructure, targeting systems such as electricity and telecommunications networks (Vatman and Hart, 2024). An investigation by Microsoft estimated that Russia employed various malware and viruses to disrupt communication systems, including (Microsoft Digital Security Unit, 2022: 3):

1. **WhisperGate/Whisper Kill** - used to manipulate data and disable systems
2. **FoxBlade** - a support tool for SonicVote weapons
3. **SonicVote** - ensures the confidentiality of FoxBlade
4. **CaddyWiper** - manipulates data and disables systems
5. **DesertBlade** - also used to manipulate data and disable systems
6. **Industroyer2** - specifically designed to attack vital infrastructure
7. **Lasainraw** - used to manipulate data and disable systems
8. **FiberLake** - employed to delete data.

According to data from the Microsoft Digital Security Unit (2022), numerous cyberattacks occurred following the Russian military invasion of Ukraine. Notably, on February 28, 2022, there were attacks on Ukrainian media, followed by data deletion incidents on March 1, 2022. A cyberattack was also directed at a Ukrainian nuclear power company on March 2, 2022. Additionally, government networks faced attacks from March 4 to March 11, 2022. In November 2023, the Ukrainian telecommunications company Kyivstar experienced a cyberattack. These various cyber-attacks have significantly disrupted the Ukrainian government's and citizens' activities, raising concerns about their security. One particularly impactful attack targeted Ukraine's infrastructure system during the winter, leading to disruptions in civilian electricity supply.

Ukraine's Strategy to Address Russian Cyber Threats

Ukraine faces a series of cyber-attacks allegedly conducted by Russia, threatening its domestic politics, energy infrastructure, social conditions, and communication activities. Therefore, the Ukrainian government must develop a comprehensive strategy to combat these Russian cyber threats and mitigate their impact. This strategy involves establishing a legal framework to ensure the security of Ukraine's cyberspace and preparing the relevant agencies responsible for maintaining that security. Additionally, as pointed out by David Alberts in Groh (2008), the Ukrainian government has integrated technological considerations into its military strategy, particularly in response to Russian cyber threats.

Ukraine's overall policy and strategy can be seen through Law No. 45, Article 403, on "*On the Basic Principles of Cybersecurity in Ukraine*" and Law No. 30, Article 258. Based on the law, Ukraine created bodies tasked with securing Ukraine's cyberspace (Verkhovna Rada of Ukraine, n.d.). These bodies include:

1. *The State Service of Special Communication and Information Protection of Ukraine.* This body is responsible for developing and implementing public policies related to cybersecurity. This organisation oversees vital players in Ukraine's cybersecurity landscape, including the State Center for Cyber Defense and the Computer Emergency Response Team (CERT).
2. *The State Center for Cyber Defense* addresses threats posed by Russian cyber activities and is authorised to investigate and respond to crimes in Ukrainian cyberspace.
3. *The Computer Emergency Response Team* (CERT) is a team that focuses on system recovery and preventive measures through comprehensive system analysis. In addition to this analysis, CERT developed a cybersecurity standard for Ukrainian cyberspace, RUSI 2023. This standard is intended to help all sectors of Ukraine, particularly the energy sector, mitigate cyberattack losses.

Establishing the CERT team and the robust legal framework supporting it have significantly contributed to Ukraine's effectiveness in countering Russian cyberattacks. Throughout 2023, the CERT team identified approximately 20 critical infrastructures targeted by cyberattacks (Computer Emergency Response Team of Ukraine, 2024). As a result, Ukraine successfully defended these 20 sites, avoiding significant cyberattack repercussions.

In addition to creating a robust legal foundation and establishing organisations dedicated to securing cyberspace, Ukraine is also enhancing its cooperation with the United States, mainly through the US Agency for International Development (USAID). A primary focus of this partnership is cybersecurity for critical infrastructure. The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity aims to bolster cybersecurity measures. Beyond protecting vital infrastructure, this collaboration seeks to transform Ukraine from a vulnerable nation into a robust player in cybersecurity. USAID has also deployed experts to identify malware and recover affected systems. These specialists help Ukrainians maintain reliable access to the internet (USAID, 2022).

Ukraine's State Service for Special Communication and Information Protection collaborates with the U.S. Cybersecurity and Infrastructure Security Agency. Given that Russia primarily targets Ukraine's vital infrastructure with cyberattacks, this partnership is focused on enhancing the security of Ukraine's cyberspace for critical infrastructure. This cooperation aims to prevent Russia from efficiently executing cyberattacks on essential systems in Ukraine. This was reaffirmed by Oleksandr Potii, who stated: "Increased real-time information sharing across agencies and critical sectors, along with committed collaboration, will help cultivate a resilient partnership" (The U.S. Cybersecurity and Infrastructure Security Agency, 2022).

Ukraine also collaborates with the U.S. Cybersecurity and Infrastructure Security Agency (CISA). As part of this partnership, the U.S. has sent experts to Ukraine to assist directly. Bryan Vorndarn, the Assistant Director of the FBI (Federal Bureau of Investigation), stated, "From the FBI's perspective, Ukraine is one of the key places where we have dedicated cyber personnel

embedded with the U.S. Government's footprint" (RSA Conference, 2023). This collaboration is particularly beneficial for Ukraine due to the U.S. Cyber Command's support in preventing cyberattacks. The U.S. Cyber Command is working closely with the Ukrainian CERT team to assess several systems that are vulnerable to potential Russian cyber operations (RSA Conference 2023).

The joint team formed between the U.S. Cyber Command and Ukraine's Computer Emergency Response Team (CERT) is called Hunt Forward (Rollins, 2023). Its primary goal is to implement preventive measures that help Ukraine minimise the impact of Russian cyberattacks. The effectiveness of this collaboration is evident in Ukraine's resilience against numerous Russian cyberattacks, especially during the military invasion in 2022. Additionally,

Ukraine's partnership with the U.S. has resulted in support from Google, which has provided 50,000 licenses to Ukrainian public officials (Google Threat Analysis Group, 2023, p. 2). These licenses are intended to enhance the security of public officials' accounts in Ukraine.

Some experts predict that cyber forces will play a more dominant role in military invasions due to a series of cyberattacks preceding the actual invasion. Sanger and Barnes (2021) noted that, prior to the invasion, Russia could leverage its cyber capabilities to assert control over Ukraine (Sanger and Barnes, 2021). However, this prediction was undermined by Ukraine's impressive resilience against Russian cyber threats. Mieke Eoyang stated that Russia was unable to fully utilise its cyber capabilities because Ukraine's cyber resilience improved (The Economist, 2022). Similarly, Microsoft indicated that Russian cyber power has had little impact on the conflict between Russia and Ukraine (Bateman, 2022: 5).

In 2023, the National Cyber Security Index (NCSI) assessed Ukraine's cybersecurity, highlighting an improvement in the country's cybersecurity capabilities. The assessment evaluates various aspects of leadership related to cybersecurity at the national level. It found that Ukraine's legal and policy frameworks received the highest ratings. This indicates that the government is responsible for national cybersecurity by enacting relevant legislation (National Cyber Security Index, 2023).

The Ukrainian government also received a positive assessment from the NCSI regarding its preparedness to face cyberattacks due to ongoing exercises and developing a comprehensive cybersecurity strategy. The effectiveness of Ukraine's periodic exercises is evident in the collaborative efforts of the CERT team and U.S. Cyber Command, which work together to address cyberattacks targeting critical infrastructure in Ukraine. Additionally, establishing well-coordinated security strategies nationally demonstrates Ukraine's commitment to enhancing its cybersecurity framework (NCSI, 2023).

CONCLUSION

Russia has utilised its cyber capabilities to undermine Ukraine even before the onset of the Russia-Ukraine War. The damage inflicted by cyberattacks can be as devastating as that caused by conventional weapons. This includes disruption to vital infrastructure, the rapid spread of disinformation, and the leakage of confidential data. In fact, cyber warfare is often seen as more advantageous for the aggressor, as the threats are more complex to detect.

In response, Ukraine is implementing strategies to bolster its cyber defences. These strategies include enhancing domestic cyber capabilities and collaborating with the United States to gain access to expert assistance in securing cyberspace. This approach has proven effective, significantly mitigating the harmful effects of Russian cyberattacks during the conflict.

Furthermore, Ukraine has established a legal framework and dedicated agencies to address cybersecurity issues. The collaboration with the U.S. has also strengthened Ukraine's resilience in this area. The Ukrainian government's rapid response team, the Computer Emergency Response Team (CERT), has been instrumental in preventing Russian cyberattacks. Cooperation with the U.S. Cyber Command has allowed Ukraine to have joint exercises to build its cyber capacity. As a result, CERT has successfully innovated Ukraine's cyber defence system (SIASPA) and improved network security across the country.

REFERENCES

1) America's Cyber Defense Agency. 2021. *Cybersecurity & Infrastructure Security Agency.* July. Accessed on April 1, 2024. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-05601.
2) Babys, Salomon A.M. 2021. "The Threat of Cyber Warfare in the Digital Era and Indonesia's National Security Solutions." *Oratio Directia* 425-441.
3) Bateman, Jon. 2022. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." *Carnegie Endowment for International Peace* 5-31.
4) Bergen, Peter, and Tim Maurer. 2014. *CNN.* March 7. Accessed on April 1, 2024. https://edition.cnn.com/2014/03/07/opinion/bergen-ukraine-cyber-attacks/index.html.
5) Berzins, Janis. 2014. *Russia's New Generation Warfare In Ukraine: Implications For Latvian Defense Policy.* Policy Paper, National Defence Academy of Latvia Center for Security and Strategic Research.
6) Computer Emergency Response Team of Ukraine. 2024. *CERT-UA.* April 19. Accessed April 23, 2024. https://cert.gov.ua/article/6278706.
7) European Parliamentary Research Service. 2022. *Russia's war on Ukraine: Timeline of cyberattacks.* European Parliamentary Research Service.

8) Fabian, Sandor.2019."The Russian hybrid warfare strategy – neither Russian nor strategy."*Defense &Security Analysis* 308-325.
9) Wired. 2022. *A Timeline of Russian Cyberattacks on Ukraine.* Accessed on April 23, 2024. https://www.youtube.com/watch?v=PWbqAV_eh7k
10) Google Threat Analysis Group. 2023. *Fog of War: How Ukraine Conflict Transformed the Cyber Threat Landscape.* Google.
11) Khan, Rafiullah, Peter Maynard, Kieran Mclaughlin, David Laverty, and Sakir Sezer. 2016. "Threat Analysis of BlackEnergy Malware for Synchrophasor Based Real-time Control and Monitoring in Smart Gird." *4th International Symposium for ICS & SCADA Cyber Security Research* 53-63.
12) Limnell, Jarno. 2018. "Russian Cyber Activities in The EU," in *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, 65-73. European Union Institute for Security Studies.
13) Miller, Christina. 2021. *Industrial Cyber Pulse.* November 11. Accessed on April 1, 2024. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attackblackenergy-attacks-the-ukrainian-power-grid/.
14) Morgus, Robert, Brian Fonseca, Kieran Green, and Alexander Crowther. 2019. "Russia and Cyberspace." *New America* 18-30.
15) Jewelry, Piret. 2018. "The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine." *Hacks, Leaks, and Disruptions: Russian Cyber Strategies* 53-64.
16) Przetacznik, Jakub, and Simona Tarpova. 2022. *Russia's war on Ukraine: Timeline of cyberattacks.* European Parliamentary Research Service.
17) Rusi. 2023. *Cyber Operations in Ukraine: A Conversation with Victor Zhora | WEBINAR SESSION 25 April 2023.* Accessed on April 27, 2024. https://www.youtube.com/watch?v=lAhw3LdkKnk
18) Rollins, Major Sharon. 2023. *U.S. Naval Institute.* June. Accessed May 1, 2024. https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessonsinside-ukraine.
19) RSA Conference. 2023. *Stronger Together: The US-Ukrainian Cyber Partnership.* Accessed May 1, 2024. https://www.youtube.com/watch?v=9w8aMo7fXrk
20) Sanger, David E., and Julian E. Barnes. 2021. *The New York Times.* December 20. Accessed May 2, 2024. https://www.nytimes.com/2021/12/20/us/politics/russia-ukrainecyberattacks.html.
21) Setiyadi, Basuki Erwin, and Makmur Keliat. 2020. "Counter Intelligence Cyber Espionage Against Democratic National Committee Members Ahead of the 2016 U.S. Presidential Election." *Journal of Strategic Studies of National Resilience* 5-18.
22) State Service of Special Communications and Information Protection of Ukraine. 2024. "Enhancement of Critical Infrastructure Protection: SSSCIP experts train sectoral specialists.
23) The Economist. 2022. *The Economist.* December 1. Accessed May 1, 2024. https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russiascyber-war-in-ukraine.
24) Vasquez, Christian, and Elias Groll. 2023. *Cyberscoop.* August 10. Accessed on April 2, 2024. https://cyberscoop.com/viasat-ka-sat-hack-black-hat/.
25) Willet, Marcus. 2022. "The Cyber Dimension of the Russia-Ukraine War." *Survival* 7-26.