TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Andrea Kivi 221881IVGM

Cyber resilience in Ukraine after beginning of Russia’s full-scale invasion

Master's thesis

Supervisor: Sille Arikas
MSc

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Andrea Kivi 221881IVGM

Küberturvalisus Ukrainas pärast Venemaa täiemahulise invasiooni algust

Magistritöö

Juhendaja: Sille Arikas
MSc

Tallinn 2025

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Andrea Kivi

Abstract

This master's thesis presents a comprehensive and analytical study of the dynamics of cyber resilience in Ukraine's complex geopolitical landscape. The aim of the research is to assess the current state of Ukraine's cybersecurity infrastructure, identify systemic vulnerabilities, and propose evidence-based strategies to enhance national cyber resilience. This study transcends mere descriptive analysis, aiming to contribute to a nuanced understanding of the interplay between cyber and conventional warfare, thereby offering valuable insights applicable to the broader cybersecurity discourse. The demands posed by the ongoing conflict have created a distinctly operational environment that necessitates a thorough analysis of the specific challenges experienced by Ukraine.

The master's thesis analyzes the evolution of cyber threat vectors targeting Ukraine's critical infrastructure, examining the strategic motives behind these attacks and their resulting impact on national stability. Furthermore, it seeks to identify existing gaps in Ukraine's cyber defence mechanisms, proposing actionable solutions based on empirical evidence and established cybersecurity frameworks. The work encompasses, but is not limited to, the evaluation of the effectiveness of technological applications, human capital development, and international cooperation initiatives.

The methodological approach involves the synthesis of qualitative and quantitative data, including the analysis of incident reports, policy documents, and expert interviews, to ensure a robust and defensible assessment. By contextualizing Ukraine's experiences within established cybersecurity theories and best practices, this research strives to generate scholarly contributions relevant to policymakers, cybersecurity practitioners, and academic researchers. The study highlights the necessity of adaptive and context-sensitive cybersecurity strategies, particularly in regions with heightened geopolitical instability.

Keywords: cyber resilience, cybersecurity, cybersecurity strategy, national security, cyber threats.

This thesis is written in English and is 63 pages long, including 6 chapters, 2 figures and 1 table.

Annotatsioon

See magistritöö esitab põhjaliku ja analüütilise uurimuse küberkerksuse dünaamikast Ukraina keerulises geopoliitilises maastikus. Uurimuse eesmärk on hinnata Ukraina küberturvalisuse infrastruktuuri praegust olukorda, tuvastades süsteemsed haavatavused ja pakkudes tõenduspõhiseid strateegiaid riikliku küberkerksuse parandamiseks. See uurimus ületab pelgalt kirjeldava analüüsi, eesmärgiga panustada nüansseeritud mõistmisse küber- ja tavapärase sõjapidamise vastastikmõjust, pakkudes seeläbi väärtuslikke teadmisi, mis on rakendatavad laiemas küberturvalisuse diskursuses. Käimasoleva konflikti poolt seatud nõudmised on loonud selgelt eristuva operatiivkeskkonna, mis nõuab Ukraina poolt kogetud konkreetsete väljakutsete põhjalikku analüüsi.

Magistritöö analüüsib Ukraina kriitilist infrastruktuuri sihtivate küberohtude vektorite evolutsiooni, analüüsides nende rünnakute strateegilisi motiive ja nende tagajärjel tekkivat mõju riiklikule stabiilsusele. Lisaks püütakse määratleda olemasolevad lüngad Ukraina küberkaitse mehhanismides, pakkudes välja rakendatavaid lahendusi, mis põhinevad empiirilistel tõenditel ja väljakujunenud küberturvalisuse raamistikel. Töö hõlmab, kuid ei piirdu, tehnoloogiliste rakenduste, inimkapitali arendamise ja rahvusvaheliste koostööalgatuste tõhususe hindamist.

Metoodiline lähenemine hõlmab kvalitatiivsete ja kvantitatiivsete andmete sünteesi, sealhulgas intsidentide aruannete, poliitikadokumentide ja ekspert intervjuude analüüsi, et tagada tugev ja kaitstav hinnang. Koondades Ukraina kogemused väljakujunenud küberturvalisuse teooriate ja parimate praktikate raames, püüab see uurimus genereerida teaduslikke panuseid, mis on asjakohased poliitikakujundajatele, küberturvalisuse praktikutele ja akadeemilistele uurijatele. Uurimus näitab kohanduvate ja kontekstitundlike küberturvalisuse strateegiate vajalikkust, eriti piirkondades, kus on suurenenud geopoliitiline ebastabiilsus.

Märksõnad: küberkerksus, küberturvalisus, küberturvalisuse strateegia, riiklik julgeolek, küberohud

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 63 leheküljel, 6 peatükki, 2 joonist, 1 tabelit.

List of abbreviations and terms

AI	Artificial intelligence
APs	Additional protocols
CERT-UA	Computer Emergency Response Team of Ukraine
CIISs	Critical Infrastructure Information Systems
CNI	Critical National Infrastructure
CNPP	Chornobyl Nuclear Power Plant
DDoS	Distributed Denial of Service
EU	European Union
FSB	Federal Security Service
IT	Information technology
ISPs	Internet service providers
NCSI	National Cyber Security Index
OECD	Organisation for Economic Co-operation and Development
PCC	Prykarpattyaoblenergo Control Center
RQ	Research Question
SSSCIP	State Service of Special Communication and Information Protection of Ukraine
SQ	Subquestion
UK	United Kingdom
US	United States

Table of contents

List of figures

List of tables

1 Introduction

On 24th of February 2022 Russia began its full-scale war of aggression against Ukraine. Physical facilities and communications infrastructure have been damaged or occupied in many areas of the country. The quality of data transmission has decreased on average by 13% over fixed internet networks and by 26% over mobile networks (OECD (2022): Digitalization for recovery in Ukraine. Policy Responses. Ukraine: tackling the policy challenges). The threat of cyberattacks waged by the Russian federation both at the Ukrainian systems and systems of the European partners remains high, since the concept of the Russian 'hybrid war' provides for using all the types of impact upon the country assaulted by Russia. The purpose of the Cybersecurity Strategy of Ukraine for 2021-2025 is to strengthen Ukraine's cybersecurity capabilities and resilience in the face of evolving cyber threats. The strategy was adopted by the Ukrainian government in December 2020 and outlines a comprehensive approach to cybersecurity that includes both defensive and offensive measures.

2023 witnessed a concentrated targeting of critical sectors in Ukraine, including media and telecommunications, central and local government institutions, the Ukrainian Defence Forces, and the defence industry. This focus on these sectors suggests a potential strategy to disrupt information flow, cripple government operations, and hinder the nation's defence capabilities (Küberturvalisuse aastaraamat, 2024). The Ukrainian cyberspace faces a significant and persistent threat emanating from the Russian Federation and associated cyber actor groups. Ukraine has experienced a significant number of Distributed Denial of Service (DDoS) attacks in recent years, particularly during times of political unrest or conflict. These attacks have targeted a wide range of organizations and infrastructure, including government websites, banks, media outlets, and critical infrastructure. In addition to this high-profile attack, Ukraine has also experienced numerous other DDoS attacks targeting government websites, media outlets, and other organizations. The trend of disruptive cyberattacks continued in December 2023 with a large-scale DDoS attack crippling the Information Technology systems of Kyivstar, Ukraine's leading mobile network operator, and Monobank, a prominent financial institution (Hunder, Landay, Bern, 2023). These attacks have often been attributed to Russian state-sponsored hacking groups or hacktivist groups sympathetic to Russia. Recognizing the gravity of the situation, Ukraine has demonstrably increased investments in cyber defence capabilities in recent years.

The aim of this study is to gain an understanding of the key factors that contribute to cyberattacks in Ukraine and analyse the Cybersecurity Strategy of Ukraine for 2021-2025. The long-term goal of this research is to contribute to a better understanding of the challenges and opportunities of cyber resilience in a wartime context. The research findings will be used to develop recommendations for how governments and organizations can build and maintain cyber resilience in the face of increasingly sophisticated and targeted cyberattacks.

The research findings will also be used to inform the development of public policies and international norms on cyber security.

To achieve these objectives, the following Research Questions (RQ) and Subquestions (SQ) were drafted:

RQ1: What are the main cyber threats and vulnerabilities in Ukraine´s public sector cyber infrastructure?

RQ2: How effective is the Cybersecurity Strategy of Ukraine for 2021-2025?

> **SQ1:** Are there any gaps in the Cybersecurity Strategy of Ukraine for 2021-2025?
>
> **SQ2:** What are the legal considerations involved in developing cybersecurity strategy?

RQ3: What are the best practices in cyber resilience from other countries?

> **SQ1:** How can they be adapted to Ukraine's context?

RQ4: How has Ukraine managed to keep e-services functioning despite being an active war zone?

> **SQ1:** How can Ukraine improve its cyber resilience against cyberattacks?

2 Theoretical framework

This chapter introduces the theory and key concepts used as the framework for the thesis. It is important to gain knowledge of existing literature, best practices and strategies adopted by other countries and an understanding of the UA strategy (strategies, policies). The collected data includes information on the frequency and severity of cyberattacks on Ukraine's critical infrastructure during the war, as well as information on the country's cyber defences measures and responses. The expected outcome is defining the theoretical framework, key areas of investigations, and knowledge about existing mitigation strategies in Ukraine. In this phase also the Cybersecurity Strategy of Ukraine for 2021-2025 will be analysed.

2.1 Concept of Cybersecurity

According to Computer Security Resource Center cybersecurity definition is following: prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (National Institute of Standards and Technology, n.d). Cybersecurity refers to defending critical systems and sensitive data against cyberattack. Cybersecurity measures, also known as information technology (IT) security, are designed to keep networked systems and applications safe from attacks that come from both within and outside a firm. E-government can refer to anything from “Online government services” to “the electronic transfer of activities and resources among individuals, companies, and other government agencies.” (Jhanjhi et al., 2022). In today's digital age, cybersecurity is vital for protecting sensitive data, mitigating cyber risks, maintaining trust, and ensuring the stability of critical infrastructure. It safeguards individuals, businesses, and societies from the growing threats in the online world. According to Craigen, Diakun-Thibault and Purse cyber security is the organisation and collection of resources, processes and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights (Craigen et al., 2014). This definition emphasizes that cybersecurity isn't just about protecting technology, it's about protecting ownership rights in the digital world.

Cyber threats appear in various forms, with motivations ranging from financial gain and regular cybercrime to state-sanctioned espionage. While classifications like cyberterrorism and cyberwarfare provide a foundation, they may not capture the evolving landscape. Organized cybercrime blurs the lines, and large-scale attacks raise questions about cyberwarfare definitions. A more nuanced system and updated legal frameworks are needed to address these complexities (Burton, 2015). A more refined classification system is needed that acknowledges the evolving nature of cyber threats and potential overlaps between categories. Furthermore, international legal frameworks should be adapted to address the complexities of cyberwarfare, particularly regarding attribution and the potential for cyberattacks to qualify as war crimes. This will require collaboration amongst governments, cybersecurity experts, and international legal scholars.

Russia's cyberattacks against Ukraine serve as a wake-up call highlighting the critical importance of cybersecurity in modern warfare. Ukraine's successful defence against a series of large scale cyberattacks, including e.g., disinformation campaigns targeting civilians, demonstrates its robust cyber resilience. However, maintaining this strength requires constant vigilance, international cooperation to share threat intelligence and best practices, and ongoing investments in bolstering cyber defences. This comprehensive approach ensures Ukraine's ability to confront and counter evolving digital threats alongside the physical challenges of the conflict.

Cyberattacks frequently target a nation's critical infrastructure and e-government platforms due to their reliance on internet and communication technologies (Abomhara, 2014). These attacks exploit vulnerabilities in software, hardware, or human behavior, potentially causing significant disruption. The severity of the attack hinges on the targeted system's importance. A highly developed e-government platform, which citizens rely on for everyday services, can be significantly crippled, hindering access to basic necessities like healthcare and essential documents (Finklea et al., 2015). Conversely, a mere informational government website may suffer reputational damage upon disruption. Including specific examples of recent cyberattacks against e-government platforms or critical infrastructure would strengthen this section. This could showcase the real-world implications of these threats and highlight the varying degrees of disruption caused by attacks on different systems.

While cyberattacks against critical infrastructure persisted throughout 2023, a notable decline in their frequency was observed compared to previous years. Ukrainian cybersecurity organizations reported 144 such attacks in the second half of 2022, which significantly dropped to 27 in the first half of 2023. This decrease suggests potential improvements in Ukrainian cyber defences or a shift in attacker tactics (Küberturvalisuse aastaraamat, 2024).

The severity of an attack depends on the targeted system and its redundancy measures. A well-designed and layered security approach can mitigate the impact of cyberattacks, but complete prevention remains a significant challenge. Destructive cyberattacks disrupt critical services, including telecommunications, finance, and news dissemination. Past examples also suggest potential for attacks on infrastructure like electricity grids (Duguin & Pavlova, 2023).

Cyberattacks become a weapon of war, disrupting lives in devastating ways. Phone lines and internet vanish, leaving people isolated and hindering emergency response. Banks and financial systems are targeted, limiting access to cash and essential services, causing economic hardship. News websites and social media platforms are compromised, creating an information blackout and potentially spreading misinformation. This passage emphasizes the elevated risk of disruptive cyberattacks targeting critical national infrastructure (CNI) in the context of hybrid operations. This includes essential services such as energy grids, water supply systems, metro networks, ports, and airports. The primary perpetrators of these attacks are suspected to be groups affiliated with Russia (State Service of Special Communications and Information Protection of Ukraine, 2024). While not yet seen in Ukraine, past cyberattacks demonstrate the chilling possibility of disrupting critical infrastructure, leading to blackouts, loss of heat, and water outages. This is the harsh reality of modern warfare, where a single cyberattack can cripple a nation's infrastructure and leave its people vulnerable.

Crippling Ukraine's energy sector has cascading effects on other parts of the economy. Cyberattacks targeting critical infrastructure facilities aim to achieve several goals: disrupting electricity distribution, stealing sensitive information, hindering data exchange, and ultimately crippling other industries that rely on these critical infrastructures (Davydiuk & Zubok, 2023).

Ukraine's experience serves as a stark reminder of the importance of robust cyber defences in today's world. Cyber resilience is not just about preventing attacks, but also about the ability to bounce back stronger from them. It is a continuous process of adaptation and improvement, crucial for any nation facing the growing threat of cyber warfare. While traditional cybersecurity focuses on technical controls and perimeter defence, a growing body of research emphasizes the concept of cyber resilience. This perspective argues that true security goes beyond prevention and emphasizes an organization's ability to adapt and recover from cyberattacks (Microsoft Security Blog, 2016).

This passage highlights a key aspect of cyber resilience: the importance of a cultural shift within IT security. As in Microsoft Security Blog (2016) suggests, simply having strong leadership and business plans is insufficient. Building a culture of security requires ongoing investment in research, education, and identifying best practices for employee behaviour. This aligns with broader discussions in organizational resilience, where cultural factors are seen as crucial for effective response and recovery.

The provided definition from the World Economic Forum papers (2012) offers a starting point for understanding cyber resilience within the IT sphere. However, it is important to acknowledge ongoing debates within the academic community regarding the precise components and optimal measurement of cyber resilience. Future research should delve deeper into effective methods for fostering a culture of security and its impact on organizational cyber resilience.

While Russia aimed to limit destructive "wiper malware" to specific Ukrainian networks in 2022, the recent and ongoing attacks were surprisingly sophisticated and widespread. Moreover, the Russian military is actively adapting these cyberattacks to the evolving war situation, even integrating them with conventional military operations (Smith 2022). It highlights the increasing sophistication, scale, and potentially coordinated nature of their attacks, which pose serious challenges for Ukraine's defence and raise concerns about the future of cyberwarfare on a global scale. Ukraine has gotten better at spotting cyber threats coming their way (thanks to AI) and has developed faster ways to protect their systems from those threats (through internet-connected security software). However, they need to keep working hard and innovating to stay ahead of potential attackers.

Ukraine's pre-war data protection law, prohibiting cloud storage for government data, proved a double-edged sword. While it may have initially aimed to protect sensitive information, it left critical infrastructure vulnerable to physical attacks (Smith, 2022).

Over the past year, Ukraine has demonstrably bolstered the cyber resilience of its critical infrastructure. This multifaceted approach encompasses both technical advancements and strategic leadership. A pivotal development was the adoption of a national plan for critical infrastructure protection in fall 2023. This plan outlines not only obligations for critical infrastructure operators and government bodies but also fosters collaboration with the private sector. This collaborative approach signifies Ukraine's recognition of the importance of a unified front in safeguarding its critical infrastructure from cyber threats (Küberturvalisuse aastaraamat, 2024).

Ukraine's foresight in recognizing this flaw and amending the law just days before the invasion proved a masterstroke. This swift action allowed them to evacuate essential data to secure cloud servers in Europe, effectively dodging the initial physical assault on government buildings. This situation highlights the importance of adaptability and flexibility in cybersecurity strategies. While strict regulations might seem secure, they can sometimes hinder necessary precautions. Striking a balance between data protection and accessibility is crucial, especially in volatile situations.

In the current technological landscape, robust cybersecurity practices are imperative for organizations that leverage computer systems, networks, and data to execute their core business functions. This necessity stems from the ever-present threat landscape posed by malicious actors, highlighting the critical need for a multi-faceted cybersecurity strategy (Shea et al., 2023). A cybersecurity strategy is not just about reacting to threats. It's a proactive approach to securing information, aligning with business goals, and building resilience against cyber threats in today's ever-evolving digital landscape.

Cybersecurity is often seen as a rigid defence aiming to prevent all attacks, while cyber resilience is viewed as an adaptive strategy that accepts some attacks are inevitable and focuses on recovering from them (Bygrave, 2022). The article's critique of a binary legal approach to cybersecurity and cyber resilience presents a compelling argument for a more holistic framework. While a purely preventative, "cybersecurity-first" approach offers a sense of security, it fails to acknowledge the evolving nature of cyber threats and the inevitability of breaches. Finding the optimal balance between prevention and preparedness will be critical in crafting effective legal frameworks that can safeguard critical infrastructure and citizen data in the face of ever-evolving cyber threats.

Effective cyber security relies on maintaining a current understanding of potential threats and continually improving preparedness to address rapid technological advancements. Cyber security policies are established to guarantee the security of Critical Infrastructure Information Systems (CIISs). These policies strike a balance between service providers adhering to state-established standards and the state's more collaborative strategy. The success of implementation hinges heavily on the willingness of third parties to comply with the new regulations. This willingness is arguably enhanced when these parties are included from the outset in the decision-making process (Weiss & Jankauskas, 2019). The ongoing war in Ukraine has thrown the nation's cyber defences into a crucible. Prior to the invasion, Ukraine had made strides in developing cyber security policies, likely benefiting from a collaborative approach that included both the government and private sector. However, the current situation presents a unique challenge.

2.2 History

In Ukraine, the Cyber Incident Response Centre documented 41 million suspicious events aimed at unauthorized interventions in information systems in 2021 alone, processing 160,000 critical events and registering 147 cyber incidents (State Service of Special Communication and Information Protection of Ukraine [SSSCIP], 2022).

Confirmed and publicly known interference has taken place in elections in the US and France, as well as in the Brexit referendum in the UK. In addition to these well-known cases, there has been systematic political interference in many countries. Cybercriminals operating under the auspices of the Federal Security Service (FSB), Russia's primary intelligence agency, engage in targeted cyber intrusions (Saar et al., 2024). Their objectives encompass a wide range of entities crucial to a functioning democracy, including legislators, journalists, universities, public sector institutions, and civil society organizations. This ongoing campaign, potentially initiated as early as 2015 in the UK case, underscores the temporal endurance of such efforts. The geographically unconstrained nature of cybercrime poses a significant challenge. The ability to launch attacks from any corner of the globe necessitates complex and multifaceted countermeasures to safeguard CNI, state institutions, and individual citizens. Collaborative efforts are crucial to fortify national defences against cyber intrusions. Educating the public about cyber threats, investing in robust cybersecurity measures for critical infrastructure, and fostering information-sharing partnerships among nations are all essential steps in this ongoing struggle. By implementing these preventative measures, democracies can bolster their resilience against the destabilizing effects of cybercrime employed as a tool of foreign policy.

The cyber dimension of the Ukraine conflict has garnered significant international attention since 2015, marked by a large-scale cyberattack that disrupted the power grid and left roughly 250,000 Ukrainians without electricity during winter. While attacks of similar scale haven't been repeated on energy infrastructure in recent years, the overall cybersecurity landscape in Ukraine remains volatile.

A 2021 report by the EU4Digital initiative (EU4Digital, 2021) highlights the significant cybersecurity challenges faced by government agencies in Ukraine. The report details the performance of government cybersecurity measures, including:

Blocked Attacks: Throughout 2021, Ukrainian government security systems successfully blocked 39,361 cyberattacks of various types.

Suspicious Events Detection: Security protocols identified 503,353 suspicious events, which can be further categorized as follows (EU4Digital, 2021):

8% of events involved attempts to gain unauthorized user credentials.

12% of events constituted attempts to escalate privileges to administrator level.

53% of events indicated violations of established corporate security policies.

The remaining 19% of events involved the detection of network spyware.

Confirmed Cyber Incidents: The Government Computer Emergency Response Team of Ukraine (CERT-UA) registered and addressed 1,960 confirmed cyber incidents during the same period (EU4Digital, 2021).

These figures, as outlined in the EU4Digital report, underscore the gravity of cyber threats not only for government institutions but also for private enterprises and individual citizens. Furthermore, the report emphasizes the critical role of securing critical infrastructure across various economic sectors in bolstering national resilience.

A notable instance of a politically motivated cyberattack transpired in January 2022, targeting the Ukrainian government (Multiple Sources). This large-scale attack involved website defacement and data deletion across various government institutions.

Specifically, the attack compromised approximately 70 Ukrainian government websites, including those belonging to the Ministries of Foreign Affairs, Defence, Energy, Education and Science (Zetter, 2022). This attack underscores the vulnerability of government infrastructure to cyberattacks. It highlights the need for robust cybersecurity measures to protect critical systems and data. Additionally, the incident raises concerns about the potential for cyberattacks to be used as a tool in geopolitical conflicts. Additionally, websites of the State Emergency Service and the Ministry of Digital Transformation, which offers public access to government services through its e-governance portal, were also affected (Zetter, 2022). The primary webpage of roughly a dozen targeted sites displayed a threatening message warning users to "be afraid and expect worse". While most websites were restored within a few days, this incident serves as a stark reminder of the vulnerabilities faced by government infrastructure in the digital age. The January 2022 cyberattack on Ukrainian government websites serves as a stark reminder of the evolving cybersecurity landscape and the need for increased vigilance and preparedness.

The geographically unconstrained nature of cybercrime poses a significant challenge. The ability to launch attacks from any corner of the globe necessitates complex and multifaceted countermeasures to safeguard CNI, state institutions, and individual citizens. Notably, the Estonian government has previously faced cyberattacks attributed to Russia, highlighting the vulnerability of smaller nations.

Beyond the direct infiltration attempts, the manipulation of information is another critical component of this anti-Western offensive. The deliberate creation and dissemination of propaganda and disinformation play a pivotal role in eroding public trust and sowing discord within targeted societies. Russia leverages both state-aligned cybercriminals and potentially private companies to amplify this disinformation campaign.

This concerning trend necessitates a robust international response. Collaborative efforts are crucial to fortify national defences against cyber intrusions. Educating the public about cyber threats, investing in robust cybersecurity measures for critical infrastructure, and fostering information-sharing partnerships among nations are all essential steps in this ongoing struggle. By implementing these preventative measures, democracies can bolster their resilience against the destabilizing effects of cybercrime employed as a tool of foreign policy.

The escalating cyberattacks that preceded Russia's full-scale invasion of Ukraine in 2022 were a chilling sign of a meticulously planned assault, not merely random or opportunistic acts. The BleedingBear attacks specifically targeted government agencies and Ukrainian websites, while the defacements with anti-Ukrainian rhetoric served as a clear indicator of their origin. This coordinated sequence, culminating in the DDoS attack and renewed BleedingBear strikes days before the invasion, suggests a deliberate strategy of cyber aggression (ESET, 2022) These attacks were more than just disruption; they were a calculated effort to sow panic, weaken Ukrainian resolve, and potentially even cripple critical infrastructure in preparation for the coming military onslaught. This coordinated cyber campaign underscores the growing importance of proactive cybersecurity measures in the face of modern warfare, where virtual battlefields can precede and complement physical ones.

The deployment of the AcidRain malware to disrupt Viasat communication modems across a vast region, encompassing Europe and the Middle East, signifies a concerning escalation. The reported disruptions in air traffic control systems in Germany and widespread internet outages highlight the far-reaching potential consequences of such attacks (Reuters, 2022). However, Ukraine's swift response, utilizing alternative satellite networks like Inmarsat and SpaceX, demonstrates remarkable resilience and adaptability in the face of a sophisticated cyber assault (Cyber Forum Kyiv, 2024).

The Viasat attack draws parallels to the infamous NotPetya cyberattack in terms of its sheer scale and indiscriminate nature. Critically, the impact extended beyond Ukraine's borders, potentially affecting civilian objects and infrastructure. This raises a crucial legal question: could such widespread cyberattacks constitute war crimes under the International Criminal Court's jurisdiction? Further investigation and legal analysis are necessary to explore this potential legal ramification.

The Viasat incident represents a paradigm shift in cyber warfare. Cyberattacks are no longer solely about disrupting military communications or intelligence gathering. They can now be employed as a precursor and force multiplier in a broader military campaign, potentially impacting civilian populations and infrastructure far from the physical battlefield. This necessitates a re-evaluation of international legal frameworks to address the potential war crime implications of such large-scale cyberattacks. Furthermore, it highlights the urgent need for enhanced international cooperation in developing robust cyber defences and fostering resilience against such novel threats.

Since the commencement of the armed conflict in Ukraine in February 2022, Russia has employed cyberattacks as a weapon against the country's strategic infrastructure. This includes documented instances of "wiper" attacks targeting government computers, financial institutions, and internet service providers (ISPs) in Ukraine (Collier, 2022). These destructive malware deployments aim to permanently erase data from compromised systems, potentially causing significant disruption and data loss. Russia's targeting of Ukrainian critical infrastructure with wiper attacks represents a reckless and irresponsible escalation in cyberwarfare. These attacks not only aim to disrupt essential services for Ukrainian citizens but also set a dangerous precedent for future conflicts. The potential for widespread data loss and cascading disruptions across critical infrastructure sectors is immense.

2.3 Cybersecurity Strategy

The Cybersecurity Strategy of Ukraine serves as a comprehensive framework outlining national priorities, goals, and objectives for safeguarding the nation's cyberspace. This strategic document aims to cultivate a secure digital environment that fosters the responsible use of cyberspace for the benefit of individuals, society as a whole, and the Ukrainian state (National Security and Defense Council of Ukraine, 2021).

Ukraine faces a complex landscape of evolving threats in the realm of cybersecurity. Here's a concise summary of the key challenges (Cybersecurity Strategy of Ukraine (2021-2025)):

1. Geopolitical Tensions and Technological Advancement:

The use of cyber tools as instruments of power in international competition creates a volatile environment. Rapid advancements in technologies like cloud computing, 5G, and AI further complicate threat landscapes and necessitate constant adaptation.

2. Weaponization of Cyberspace:

The growing sophistication of cyber weapons raises concerns about covert attacks, manipulation of critical infrastructure, and potential societal disruption.

3. Evolving Attack Methods:

Malicious actors increasingly leverage social engineering, AI, and cryptocurrencies to target individuals and systems, demanding robust defences.

4. Pandemic-Driven Vulnerabilities:

The pandemic's reliance on remote work and online services has amplified vulnerabilities in cyberspace, potentially leading to data breaches and privacy violations.

These interconnected challenges require a multi-faceted approach to strengthen Ukraine's cybersecurity posture. The outlined challenges paint a concerning picture for Ukrainian cybersecurity. The document highlights a confluence of factors creating a perfect storm. Geopolitical tensions fuel cyber aggression, while rapid technological advancements provide new avenues for attacks. This is further complicated by the increasing sophistication of cyber weaponry and the evolving tactics of malicious actors.

The pandemic adds another layer of complexity. The shift to remote work and online services has created new vulnerabilities that attackers can exploit. This could lead to significant disruptions in essential services and potential privacy violations for Ukrainian citizens.

The good news is that by acknowledging these challenges, Ukraine can begin to address them. A comprehensive cybersecurity strategy that prioritizes proactive measures like threat intelligence, infrastructure hardening, and user education can be crucial in mitigating these risks. International cooperation in sharing best practices and fostering collective defence mechanisms would also be highly beneficial. Overall, while the challenges facing Ukraine's cybersecurity are significant, they are not insurmountable.

By taking decisive action, Ukraine can build a more resilient cyberspace and protect its critical infrastructure, economy, and citizens.

Ukraine's Cybersecurity Strategy presents a positive roadmap, but its successful implementation hinges on overcoming resource constraints, bridging the digital literacy gap, and securing international support.

Ukraine faces a relentless struggle against cyberattacks targeting its critical infrastructure. These attacks form a central pillar of the wider hybrid war waged by Russia against Ukraine. The energy grid, encompassing oil, gas, nuclear, electricity, and hydroelectric systems, stands as a prime target for these attacks, highlighting their strategic intent. According to the State Service of Special Communications and Information Protection of Ukraine, there were 2.8 times more cyber incidents in Ukraine in 2022 than in 2021. The Report of the State Cyber Protection Center demonstrates that the total number of critical information security events, originating from russian IP addresses, has grown by 26% as compared to 2021 (United Nations, 2023). On National Cyber Security Index Ukraine is on 4th position and 78th on Global Cybersecurity Index. The National Cyber Security Index is a global live index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cyber security capacity building.

Ukraine's quick response to a pre-existing vulnerability demonstrates the importance of proactive cybersecurity measures. Their success serves as a valuable lesson for other nations to constantly evaluate and adapt their defence strategies. News reports indicate that Ukraine has entrusted some government data to a private cloud storage facility located in Poland. This specific server is dedicated solely to Ukrainian data, with all further details surrounding this arrangement remaining confidential. Notably, Poland represents the first partner in this initiative, and Ukraine is reportedly in talks to establish similar cloud storage agreements with other nations, including Estonia and France (Satter & Pearson, 2022).

Critical infrastructure refers to the systems, facilities, and assets that are considered essential for the functioning of a society and economy. Governments typically have plans and regulations in place to protect critical infrastructure from these threats. Cyberattacks on critical infrastructure are now standard issue. The annexation of Crimea by Russia in

2014 marked a turning point in the use of cyberattacks as a tool of statecraft. Russia employed cyber operations of varying scale and complexity, targeting Ukrainian government institutions, military networks, information systems, and critical infrastructure (Brumfield, 2022). These attacks continued even after the military conflict subsided.

The Geneva Conventions and their Additional Protocols (APs) establish a cornerstone framework for the protection of civilians and civilian objects during armed conflict. While the term "critical infrastructure" is not explicitly defined within these legal instruments, a closer examination reveals an implicit framework for safeguarding essential civilian systems and locations (Newbill, 2019). The Geneva Conventions offer a valuable yet nuanced framework for protecting civilian infrastructure during armed conflict. While the term itself may not be explicitly used, the Conventions provide a foundation for safeguarding essential services and preventing civilian harm. However, ongoing advancements in technology and the evolving nature of warfare necessitate continued dialogue and potential revisions to ensure the continued effectiveness of these legal protections.

A notable instance occurred in December 2015, when a suspected Russian cyberattacker gained control of the Prykarpattyaoblenergo Control Center (PCC) in western Ukraine. This attack resulted in power outages for approximately 230,000 people, lasting up to six hours (Wagner, 2016). It highlights the vulnerability of critical infrastructure to cyberattacks and the potential for widespread disruption. This incident underscores the urgent need for robust cybersecurity measures to protect these vital systems. Additionally, it emphasizes the importance of international cooperation in attributing and deterring such attacks. The lack of clear international legal frameworks regarding cyberwarfare further complicates the issue.

Assumption that this attack potentially originated from Russia raises additional concerns. It suggests a willingness to employ cyberattacks not just for espionage or disruption, but also to inflict harm on civilian populations. This chilling development necessitates a re-evaluation of international norms and potential consequences for such actions.

Over 40% of recent destructive cyberattacks in Ukraine targeted critical infrastructure sectors, posing a significant threat beyond immediate damage. Areas like power grids, communication networks, and essential services could be crippled, causing cascading negative effects on the government, military, economy, and civilians. This highlights a deliberate strategy by attackers to maximize disruption. Additionally, a concerning 32% of these attacks directly targeted Ukrainian government organizations at various levels. This suggests a coordinated attempt to cripple the nation's ability to respond effectively. (State Service of Special Communications and Information Protection of Ukraine. 2024). Overall, the targeting of critical infrastructure and government institutions paints a grim picture of the sophistication and ruthlessness of cyberattacks against Ukraine. It underscores the importance of robust cyber defences, international collaboration in threat intelligence sharing, and the need to stay ahead of constantly evolving cyber threats.

The full-scale invasion of Ukraine by Russia in February 2022 raised significant concerns about the safety and security of the country's nuclear power plants, particularly the decommissioned Chornobyl Nuclear Power Plant (CNPP). The capture of the CNPP by Russian forces on February 24th, 2022, and subsequent disruptions to its power supply introduced a potential nuclear safety crisis (Guchua & Zedelashvili, 2022).

On March 9th, 2022, Ukrenergo, the Ukrainian national electricity grid operator, reported a complete loss of external power supply to the CNPP. Ukrenergo attributed this outage to damaged power lines caused by ongoing fighting north of Kyiv, further hindering repair efforts (Guchua & Zedelashvili, 2022).

The loss of external power supply raised concerns about the potential spread of radioactive material across Ukraine, Russia, Belarus, and Europe, as highlighted by Ukrenergo's statement (Guchua & Zedelashvili, 2022). Additionally, the presence of approximately 210 Ukrainian technical staff and security personnel at the CNPP under Russian control added a layer of human resource risk to the situation.

The Russian invasion of Ukraine significantly heightened nuclear safety concerns surrounding the CNPP. The loss of external power and the presence of a potentially compromised workforce introduced serious potential risks for a radiological release. Beyond Chornobyl, Russia's capture of the Zaporizhzhia Nuclear Power Plant on March 3rd, 2022, raised further safety concerns. Though a fire was extinguished and radiation levels remained stable, the incident highlighted the vulnerability of Ukrainian nuclear facilities (Guchua & Zedelashvili, 2022).

Furthermore, cyberattacks targeted Ukrainian critical infrastructure and strategic facilities, while Iranian drones damaged energy infrastructure, amplifying the overall dangers faced by Ukraine. These events underscore the critical importance of international cooperation and protocols in ensuring the safety and security of nuclear facilities during periods of armed conflict.

Russia's cyber operations in Ukraine are not just collateral damage; they are a calculated and ruthless strategy to cripple Ukraine's defences and manipulate the information landscape. This approach underscores the need for a strong international response to deter further attacks and protect critical infrastructure globally (Figure 1).

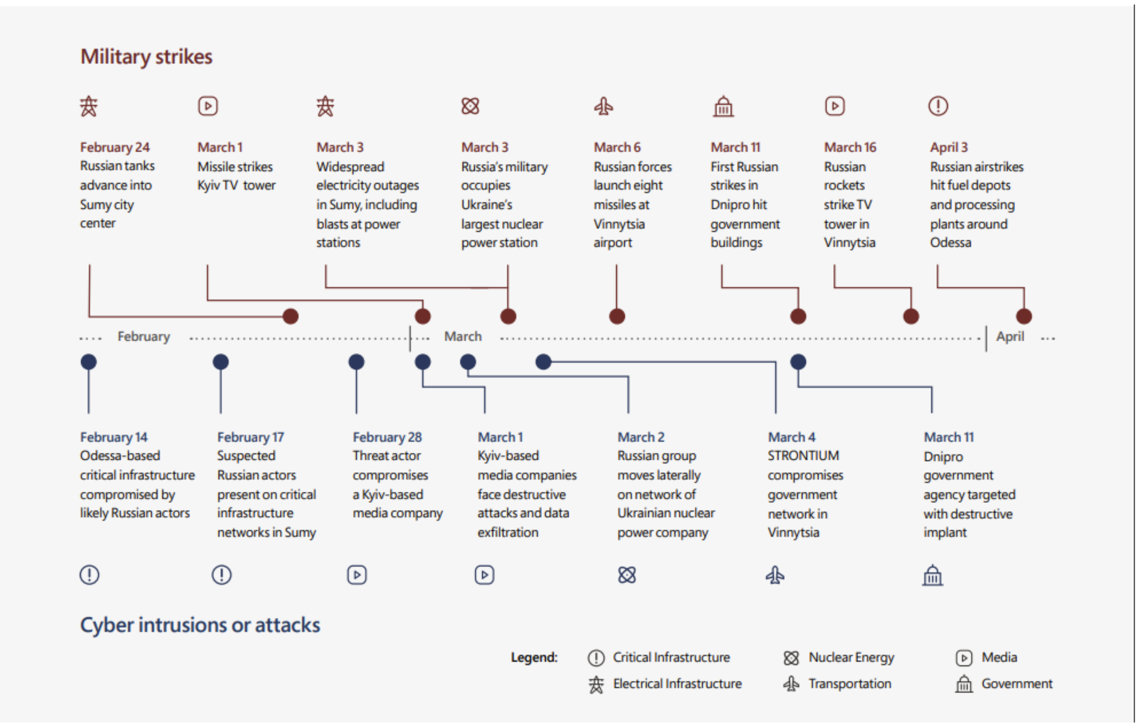
Military strikes
February 24 Russian tanks advance into Sumy city center
March 1 Missile strikes Kyiv TV tower
March 3 Widespread electricity outages in Sumy, including blasts at power stations
March 3 Russia's military occupies Ukraine's largest nuclear power station
March 6 Russian forces launch eight missiles at Vinnytsia airport
March 11 First Russian strikes in Dnipro hit government buildings
March 16 Russian rockets strike TV tower in Vinnytsia
April 3 Russian airstrikes hit fuel depots and processing plants around Odessa
February
March
April
February 14 Odessa-based critical infrastructure compromised by likely Russian actors
February 17 Suspected Russian actors present on critical infrastructure networks in Sumy
February 28 Threat actor compromises a Kyiv-based media company
March 1 Kyiv-based media companies face destructive attacks and data exfiltration
March 2 Russian group moves laterally on network of Ukrainian nuclear power company
March 4 STRONTIUM compromises government network in Vinnytsia
March 11 Dnipro government agency targeted with destructive implant
Cyber intrusions or attacks
Legend:
Critical Infrastructure
Electrical Infrastructure
Nuclear Energy
Transportation
Media
Government

Figure 1. Military strikes

A web of cyber threats is ensnaring Ukraine's critical infrastructure, particularly its energy sector, which acts as the lifeblood of the entire economy. The information gleaned from these attacks goes beyond mere disruption. It can be used to plan targeted missile strikes, increasing the potential for devastating physical damage and loss of life. Furthermore, disrupting information exchange acts as a distraction, masking the attacker's true objectives and allowing for more significant system infiltration (Davydiuk & Zubok, 2023).

The increasing sophistication of these cyberattacks, coupled with the vulnerability of energy companies' supply chains, presents a major concern. Detecting and defending against these complex threats requires robust cybersecurity measures implemented not only by individual companies but also throughout the entire supply chain. The cyberattacks on Ukraine's energy sector highlight the interconnectedness and vulnerability of critical infrastructure in today's digital age (Figure 2). These attacks require a multi-pronged approach, encompassing strengthened defences, international cooperation, and proactive measures to address supply chain vulnerabilities. Ignoring these threats could have devastating consequences for Ukraine and set a dangerous precedent for future cyber conflicts.

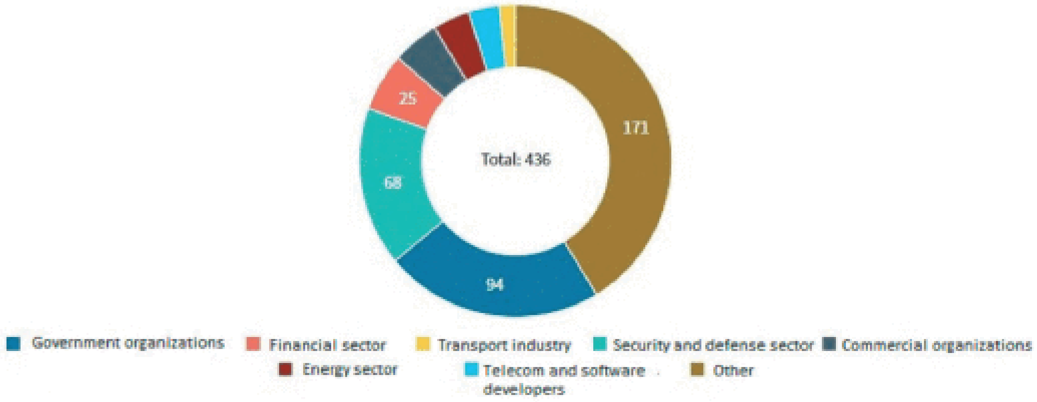

Figure 2. Cyberattacks

One of the most impactful cyberattacks since the start of the invasion occurred in March 2022 against Ukrtelecom, Ukraine's largest telecom company, leaving nearly 80% of customers without internet for hours. Other, smaller cyberattacks have also targeted the telecommunications sector, and of course, direct military action has also caused service disruptions. This made it difficult to recover from some cyberattacks, as physical access to some equipment was required, but this would have been life-threatening for workers due to the fighting (Küberturvalisuse aastaraamat, 2023). Cyberattacks have been a major part of the Russian invasion of Ukraine, targeting critical infrastructure like telecommunications and energy. These attacks have had a significant impact on the Ukrainian people and economy, and they highlight the need for strong cybersecurity measures in the face of modern warfare. However, the continued targeting and the challenges posed by physical access during wartime highlight the urgent need for robust cybersecurity measures and international cooperation to defend against these attacks.

Ukraine's success in maintaining critical services despite a surge in cyberattacks is a testament to their remarkable cyber resilience. The combined efforts of their own robust defences, international support from countries and IT companies, and the valuable experience gained from past cyberattacks since 2014 have proven highly effective (Küberturvalisuse aastaraamat, 2023). The country's digital services remain operational, and cyberattacks have not caused disruptions to water, electricity, or other essential services. These disruptions have been mainly caused by kinetic warfare.

In addition to Ukraine's own capabilities, it has received assistance in the cyber domain from both countries and several global IT and cybersecurity companies. According to the Ukrainian Security Service (SSU), over 4,500 cyberattacks were successfully blocked in 2022, which is more than five times the number of attacks documented in 2020 (800).

This situation showcases several crucial points:

Preparedness is Key: Ukraine's long history of being a target for cyberattacks allowed them to anticipate and develop strong defences.
International Cooperation Matters: The assistance from other countries and IT companies demonstrates the power of collaboration in bolstering cybersecurity during a crisis.
Cybersecurity is National Security: The disruption of critical services like water and electricity highlights the importance of cybersecurity as a fundamental pillar of national security.

This example serves as a valuable lesson for other nations to invest in robust cybersecurity measures and foster international cooperation to counter the growing threat of cyber warfare.

As the war intensified, Russia escalated its cyberattacks, specifically targeting Ukraine's CNI. In February, they attempted a major disruption by infiltrating one of Ukraine's largest energy facilities. This attack, planned for April 8th, aimed to utilize the same tactics used in previous cyberattacks against Ukraine in 2015 and 2016. However, Ukrainian cybersecurity forces successfully neutralized the threat (Willett, 2022).

In late April 2022, Microsoft reported that it had tracked more than 237 Russian cyber operations against Ukraine since just before the invasion, and that some had been successful, with ‘nearly 40 discrete destructive attacks that permanently destroyed files in hundreds of systems across dozens of organisations in Ukraine (Smith, 2022).

Russia's escalating cyberattacks on Ukraine's critical infrastructure are deeply concerning, not just for the immediate damage they can cause, but for their potential to become a terrifyingly integrated aspect of modern warfare. The targeting of energy facilities and the attempt to disrupt media organizations during a physical attack on Kyiv's TV tower showcase a deliberate strategy to cripple essential services and manipulate information flow. Additionally, the breach of a nuclear power company's network coinciding with a physical occupation raises serious questions about potential nuclear safety risks.

Microsoft's observations about these coordinated attacks highlight the increasing convergence of cyber and physical warfare. This poses a significant challenge, as it requires not only robust cyber defences but also a re-evaluation of traditional military strategies to account for this new integrated approach (Smith, 2022).

The international community needs to take a strong stance against these tactics. Collaborative efforts are crucial to strengthen Ukraine's cyber defences, deter further attacks, and establish clear international norms against weaponizing cyberattacks in a way that could have catastrophic consequences.

The IT Army of Ukraine was formed on 26 February by Mykhailo Fedorov, Deputy Prime Minister of Ukraine and Minister of Digital Transformation, via his Twitter account. It uses a Telegram channel to pass on instructions and list both domain names and IPs of Russian systems that the group wishes to ‘target’. It encourages people from anywhere to help the Ukrainian cause by performing DDoS attacks or other exploits against the listed sites. (O’Connor, 2022)

The digital age has made cybersecurity a cornerstone of national security. Without it, e-governance and basic state functions are crippled. Cyberattacks, a growing threat, inflict billions in damages on individuals, businesses, and governments daily (Braman et al., 2014). Leading nations prioritize national cybersecurity strategies to identify and mitigate these risks. International cooperation is key. However, a scientific approach is crucial. Understanding and minimizing cyber threats can significantly lessen their impact. The Russia-Ukraine war exemplifies this – cyberspace threats can disrupt war efforts. In essence, robust cybersecurity strategies and international cooperation are essential to defend against the growing and pervasive threat of cyberattacks in today's interconnected world.

While Russia launched a multi-pronged attack on Ukraine, the cyber dimension hasn't yielded the decisive advantage some expected. Ukraine's response demonstrates a crucial point - cybersecurity is no longer an optional extra, it's a vital line of defence (Lagvilava, 2023). By learning from Ukraine's experience, the international community can build stronger defences and work together to mitigate the growing threat of cyberwarfare.

As evidenced by their comprehensive cyber defence strategy employed between 2014 and 2022, Ukraine had been anticipating a cyber assault from Russia for years (Fahim, 2023). This proactive approach, documented in a 2016 National Cybersecurity Strategy (NCSS), prioritized data redundancy, enhanced encryption, and instilled basic cyber hygiene practices within the nation (Nehrey et al., 2022). Additionally, Ukraine collaborated with external organizations to establish real-time monitoring of critical infrastructure networks and systems. They further bolstered their defences by relocating data and essential services outside of Ukraine's borders. These measures significantly bolstered Ukraine's ability to defend against cyber and kinetic attacks, hindering Russia's ability to orchestrate and execute successful offensives (Gavrila, 2022). It's crucial to acknowledge that the thwarted Russian cyberattacks were not a result of a lack of effort on their part, but rather a testament to the tenacity of the Ukrainian defence, fortified by nearly a decade of Western support. For other countries, directly replicating Ukraine's strategy might not be entirely feasible. However, the core principles behind their success – data redundancy, robust encryption, and a culture of cyber hygiene – are universally applicable

2.4 Developing National Cyber Strategy

2.4.1. The Complexities of National Cyber Defence Strategy

The formulation and execution of a national cyber defence strategy presents a significant challenge due to the multifaceted nature of the cyber policy ecosystem. This ecosystem is characterized by a complex interplay of diverse agencies, actors with potentially conflicting interests, and entrenched positions on cybersecurity issues (Lindström et al., 2021). The formulation and execution of national cyber defence strategies present a significant challenge for nation-states in the contemporary digital age. This complexity arises from a confluence of factors that demand a multifaceted analysis. Cybersecurity's multifaceted nature demands collaboration between civil stakeholders from diverse sectors. This ensures comprehensive policies that address the vast range of cyber threats and concerns (Ertan et al., 2020). It means that different people have different pieces of the cybersecurity puzzle. By working together, they can create a more complete picture and develop effective strategies to protect everyone in cyberspace.

2.4.2. The Role of National Cybersecurity Strategies

A systematic approach for nations to tackle cyberspace challenges is the development of a NCSS. Many countries, large and small, have already implemented NCSSs, with regular updates (typically every 3-5 years) to reflect the evolving threat landscape (as evidenced by the National Cyber Security Index and the International Telecommunication Union). The development of National Cybersecurity Strategies (NCSS) represents a well-established approach for states to systematically address the challenges emanating from cyberspace (National Cyber Security Index, n.d.; International Telecommunication Union, n.d.).

2.4.3. The Importance of International Cooperation in NCSS

A critical element within NCSS frameworks is the emphasis on cooperation at the regional and international levels (NCS Guide, 2021, pp. 5, 50-53). This focus on international cooperation is driven by several key factors.

Firstly, the transnational nature of cyber threats necessitates a coordinated global response. Osula and Kaska (2013, p. 17) highlight the need for "international cooperation and coordination of activities," given that cyber threats disregard national borders. This collaborative approach is particularly crucial for smaller states, whose security often hinges on stability, predictability, and a collective response to international challenges (Brady & Thorhallsson, 2021). Neuneck (2013, p. 92) further emphasizes the importance of international cooperation in mitigating the potential for future cyber conflict.

Secondly, smaller states often face resource limitations compared to their larger counterparts. This necessitates seeking protection and assistance from international organizations. Through such partnerships, smaller states can leverage the combined resources and expertise of the international community. Furthermore, membership in international organizations offers smaller states a platform to influence global cybersecurity agendas in their favor (Crandall, 2014, p. 32; Bailes et al., 2016, pp. 1, 5).

NCSS frameworks that prioritize international cooperation are essential for effectively addressing the multifaceted challenges of cyberspace. This collaborative approach is particularly vital for smaller states, leveraging collective resources and expertise to enhance their cybersecurity posture.

2.4.4. The European Union's Cybersecurity Framework

The European and Euro-Atlantic context exemplifies the benefits of international cooperation in cybersecurity. Institutions like the EU and NATO provide frameworks for smaller states to engage with larger ones on an equal footing, fostering collaboration and knowledge transfer (Crandall, 2014).

The EU's approach to cybersecurity is guided by two key documents:

- Cyber Security Strategy for the Digital Decade (2020): This strategy outlines the EU's vision for a secure cyberspace in the coming years (The EU’s cybersecurity strategy for the digital decade, Publications Office, 2020)
- Cyber Defence Policy (2022): This policy strengthens the European Union's (EU) ability to respond to cyberattacks and foster cooperation among member states (European Commision, 2022).

The EU's primary cybersecurity agency is the European Agency for Cybersecurity (ENISA). ENISA collaborates with member states and other EU bodies, focusing on capacity building and raising cybersecurity awareness.

The EU's engagement in cybersecurity also occurs within the Common Security and Defence Policy (CSDP) framework. The CSDP allows the EU to utilize civilian, police, and military resources for crisis prevention, management, and post-crisis rehabilitation (Federal Foreign Office. (n.d.)).

Permanent Structured Cooperation (PESCO): This CSDP component offers a legal framework for member states to collaborate on specific defence areas, including cybersecurity. The European Defence Agency facilitates these cooperative efforts (PESCO projects adapt and accelerate amid shifting European security landscape, EU report finds, 2023). The 2021 EasternPartnership Summit highlighted the need for enhanced CSDP cooperation (European Parliament, 2022).

PESCO enables the EU to deploy cybersecurity experts from member states to assist partner countries in crisis situations (Duguin & Pavlova, 2023).

Network and Information Security Directive (NIS Directive):

This critical EU legal instrument establishes EU-wide cybersecurity rules. The initial 2016 directive focused on developing NCSSs, establishing national CSIRTs (Computer Security Incident Response Teams), and notification requirements for essential service providers (Kert-Saint Aubyn, M. (n.d.), 2016).

This overview demonstrates the comprehensive framework the EU has established for cybersecurity. Furthermore, it highlights the potential for collaboration between the EU and Ukraine particularly in the context of PESCO and the NIS2 Directive.

2.4.5. Ukraine's Wartime Digital Mobilization: Adaptability and Strategic Planning

In a groundbreaking move during wartime, Ukraine became the first nation to successfully migrate critical and sensitive data to cloud services located outside its borders (Aviv & Ferri, 2023). Facing a desperate situation in the war's early months, Ukraine embraced any assistance it could get. Tech giants like Microsoft, Amazon, and Google provided crucial cyber and cloud services. Elon Musk's Starlink terminals offered vital communication channels. Facial recognition software came from Clearview AI, while startups and major defence companies alike contributed experimental drones, cameras, and jamming equipment (Bergengruen, 2024). The Ukrainian case study highlights the importance of striking a balance between adaptability and strategic planning. While the initial willingness to embrace any available assistance was crucial in the early stages of the war, long-term success hinges on developing a more systematic approach. This could involve fostering closer collaboration with tech partners to develop standardized solutions, prioritizing the integration and training on proven technologies, and establishing clear protocols for evaluating and deploying experimental tools. As Alex Bornyakov, Ukraine's Deputy Minister of Digital Transformation, aptly stated, there was initially "no process," just the necessity to accept any available tool to counter the Russian threat. However, by summer, Bornyakov acknowledged the need for a more strategic, long-term approach (Bergengruen, 2024). The Ukrainian digital mobilization serves as a compelling example of how rapid adaptation can be a powerful tool in modern warfare. However, achieving long-term success necessitates a shift from a purely reactive approach towards a more strategic one. By integrating adaptability with long-term planning, Ukraine can ensure its digital arsenal remains a potent force in the ongoing conflict.

Reports highlight Ukraine's impressive ability to defend against Russian cyberattacks. This success likely stems from a two-pronged approach: a NCSS emphasizing data redundancy and resilience, and a public-private partnership providing crucial guidance, training, and remote monitoring. This collaborative effort, alongside international support for Ukraine's cyber defences, is believed to be a significant factor behind the limited impact of cyberattacks in the conflict (Gavrila, 2022).

2.4.6. Enhanced EU-Ukraine Cybersecurity Cooperation Post-Invasion

After the full invasion of Russia to Ukraine cybersecurity cooperation between Ukraine and the EU has been significantly strengthened. The European Union Agency for Cybersecurity (ENISA) further solidified cooperation by signing a working arrangement with Ukraine in November 2023, building upon the established EU-Ukraine Cybersecurity Dialogue. This agreement fosters a structured framework for continued collaboration and knowledge exchange in the realm of cybersecurity (European Union Agency for Cybersecurity, 2023).

The surge in cooperation manifests through several novel support mechanisms. Notably, the PESCO project, "Cyber Rapid Response Teams" (CRRTs), witnessed activation to assist Ukraine in February 2022 (European Parliament, 2022). This initiative exemplifies the swift operationalization of PESCO capabilities in response to real-world threats. Furthermore, sources suggest preparations for a potential second deployment of CRRTs in 2023 (Grossman, 2023). Beyond rapid response teams, the EU actively funded a dedicated project titled "EU Support to Strengthen Cyber Security in Ukraine" from March 2022 to February 2023. This project, boasting a budget exceeding €10 million and implemented by e-Governance Academy, targeted critical areas like secure public service delivery, critical infrastructure protection, and equipment provision for Ukrainian state authorities (e-GA). The aim of this project was to protect the databases and networks from cyber threats and secured data confidentiality, integrity and availability for the government information systems and critical infrastructure. As a result, access to public services was granted during the war, cyber resilience and data protection were improved, and critical infrastructure was protected. This initiative demonstrates the EU's commitment to long-term capacity building in Ukraine's cybersecurity posture.

2.5 Tallinn Mechanism

Ukraine needs extensive multi-year assistance to maintain and strengthen its cybersecurity and cyber resilience capabilities in the face of continued destruction of the country's critical infrastructure and obstacles to the provision of vital services caused by Russian cyber operations (Välisministeerium, s.a.). The purpose of the mechanism is to pool activities with which members support the development of civilian cyber capabilities, to help integrate/coordinate this activity with other relevant areas of international assistance to Ukraine, and with the overall greater situational awareness (Välisministeerium).

The Tallinn Mechanism is a proactive effort to bolster Ukraine's cybersecurity defences. It will actively coordinate international assistance, focusing on three key areas: strengthening Ukraine's cyber resilience, safeguarding its critical infrastructure, and countering Russian cyber operations. Recognizing the importance of collective action, the Mechanism's members aim to improve collaboration in delivering civilian cyber capacity building programs. To achieve these goals, they plan to engage with the EU and NATO, while also welcoming contributions from the private sector and non-governmental organizations.

Conducting cyber exercises specifically designed for decision-makers at the political level, both within the EU and the North Atlantic Treaty Organization (NATO), is recognized as a highly effective method for raising awareness of the potential consequences of cyberattacks (CISA Insights, 2022). These exercises can simulate real-world scenarios, allowing decision-makers to experience the complexities of responding to a cyber incident in a controlled environment. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) underscores the crucial role of strategic-level cyber exercises for decision-makers (Cho et al., 2021). Exercises that incorporate strategic decision-making elements are essential for building cyber resilience, as indicated in the lessons learnt of the CCDCOE's annual "Locked Shields" exercise.

The report by NATO CCDCOE emphasizes the interconnected nature of national security and robust network defence for critical infrastructure. Furthermore, it underscores the fact that cyber resilience is not solely a technical issue. Effective translation of national cybersecurity strategies into actionable policies and procedures requires a comprehensive understanding by all stakeholders, including political decision-makers.

3 Methodology

The study uses case study approach. The study will begin with a literature review to identify the most significant cyber threats and vulnerabilities facing Ukraine. The case study has exploratory, explanatory and descriptive elements. It will also assess the existing cybersecurity policies, regulations, and frameworks in Ukraine and compare them with international best practices. The document analysis will focus on identifying the key cyber threats and vulnerabilities that Ukraine faces during the war, the steps that Ukraine has taken to build its cyber resilience, and the lessons that can be learned from Ukraine's experience.

Next are interviews with cyber security experts and government officials. The methodological design of this study incorporated semi-structured interviews as a primary qualitative data collection technique. An interview guide, consisting of open-ended questions, was developed to facilitate an in-depth exploration of participant experiences. This approach, characterized by its inherent flexibility, enabled iterative probing and the identification of salient thematic constructs, which were then subjected to a rigorous thematic analysis. The data will be analysed. Ethical considerations were considered throughout the research process. Informed consent was obtained from all participants in the expert interviews. Confidentiality will be maintained for all participants and data collected. Ensuring the safety and privacy of research participants is paramount, particularly in conflict-ridden areas. This necessitates employing secure communication channels, anonymizing data, and implementing robust data storage practices. Research focused on enhancing cybersecurity could inadvertently provide malicious actors with information about vulnerabilities in Ukrainian systems. It is crucial to recognize this possibility and implement measures to minimize its impact, such as restricting the scope of research and divulging findings only to trustworthy collaborators. The interviewee affiliations are presented in Table 1. In total, four interviews were conducted. 4 interviews we conducted in Kyiv during the visit from 23-30.03.2025 in person. During the interviews the answers were written, followed by manual proofreading and correcting to get a clear, edited text. The semi-structured interview consisted of 15 questions that are presented in Appendix 2.

Table 1. Interviewee Affiliations

Interviewee	Position
Valery Tsiupa	Co-Founder and President - International Cyber Academy
Roman Sologub	CEO - Information Systems Security Partners
Kostyantyn Ryzhkov	Program Manager - Information Systems Security Partners
Ihor Malchenyuk	Director of the Cyber Defence Department Administration of the State Service for Special Communications and Information Protection of Ukraine

The transcripts were reviewed several times to become familiar with the data and uncover initial ideas and concepts. After the initial data familiarisation stage, a coding framework was developed, which involved identifying significant phrases, words or sentences within the data. These codes were organised into categories, and categories were then refined and organised into themes that captured broader patterns within the data. Next, the themes were reviewed and refined through an iterative process until the final themes accurately represented the data and addressed the research questions.

The study combines qualitative data collection and analysis, case-studies (this will involve conducting in-depth case studies of specific cyberattacks and responses in Ukraine), semi-structured interviews with the cyber security experts, government officials and policy makers. Qualitative research is an approach for exploring and understanding the meaning individuals or groups ascribe to a social or human problem. The process involves emerging questions and procedures, data typically collected in the participants´s setting, data analysis inductively building from particulars to general themes, and the researcher making interpretations of the meaning of the data (Crewswell, 2014). This approach involves identifying common themes and patterns in the data. The thematic analysis will be used to answer the research questions and develop recommendations for how governments and organizations can build and maintain cyber resilience in the face of increasingly sophisticated and targeted cyberattacks.

4 Results

The following chapter will give the results to the research questions.

4.1 Main cyber threats and vulnerabilities in Ukraine

RQ1: What are the main cyber threats and vulnerabilities in Ukraine´s public sector cyber infrastructure?

- The Ukrainian cyberspace faces a significant and persistent threat emanating from the Russian Federation and associated cyber actor groups.

- Ukraine has experienced a significant number of DDoS attacks in recent years, particularly during times of political unrest or conflict.

- These attacks have targeted a wide range of organizations and infrastructure, including government websites, banks, media outlets, and critical infrastructure.

- Vulnerabilities include susceptibility to wiper attacks, which aim to erase data from compromised systems.

Ukraine's experience during the ongoing conflict has transformed it into a critical case study for understanding the evolving nature of cyber warfare. The shift from targeted propaganda attacks to disruptions of essential services like energy and transportation underscores the strategic intent to destabilize society and inflict human suffering. The vulnerabilities exposed in Ukraine's critical infrastructure, particularly the exploitation of third-party service providers, highlight the interconnectedness of modern systems and the need for comprehensive security measures. Building robust cyber resilience requires a multi-faceted approach, encompassing advanced threat detection, rapid incident response, and continuous data recovery capabilities. Crucially, addressing the acute shortage of qualified cybersecurity personnel and prioritizing human factor training are paramount. International collaboration plays a vital role in bolstering Ukraine's defences, offering valuable lessons for global cybersecurity strategies. The recognition that cyberattacks are integral to hybrid warfare necessitates a holistic security framework that integrates physical and digital protection. Ultimately, Ukraine's struggle emphasizes the urgent need for nations to adapt and innovate in their cybersecurity strategies to safeguard critical infrastructure and maintain societal stability in an increasingly interconnected and volatile digital landscape.

A significant pattern observed in the cyberattacks against Ukraine is the consistent targeting of critical infrastructure sectors, particularly the energy and finance industries. This focus underscores the strategic importance of these sectors for maintaining national stability and functionality. Various types of attacks have been identified, including those attributed to sophisticated Advanced Persistent Threat (APT) groups, known for their long-term and targeted campaigns, and potentially state-sponsored actors, indicating a high level of organization and resources behind these operations.

The principles of zero trust, emphasizing the need for continuous verification and limiting access, and the paramount importance of resilience, characterized by continuous readiness and robust defence mechanisms, have been highlighted as crucial for mitigating these threats. The cyberattack on DIIA (Ukrainian digital services platform) serves as a stark example of attempts to disrupt essential public services, underscoring the critical need for redundancy and distributed architectures to avoid single points of failure in critical national infrastructure.

The ongoing operation of essential services such as energy, transportation, and healthcare amidst war-induced disruptions inherently makes them attractive targets for cyberattacks. The vulnerability of these sectors likely stems from their critical nature for societal functioning, the vast amounts of sensitive information they manage, and their potential to cause widespread disruption and cascading effects if compromised.

4.2 Ukraine´s Cybersecurity Strategy efficiency

RQ2: How effective is the Cybersecurity Strategy of Ukraine for 2021-2025?

- The Cybersecurity Strategy of Ukraine for 2021-2025 aims to strengthen Ukraine's cybersecurity capabilities and resilience in the face of evolving cyber threats.

- The strategy outlines a comprehensive approach to cybersecurity that includes both defensive and offensive measures.

- The effectiveness of the strategy is analyzed in the thesis, considering the context of the ongoing conflict and evolving cyber threats

Initially, in the years leading up to the full-scale invasion, cyberattacks primarily targeted the homepages of various organizations with the aim of leaking as much data as possible.

This initial phase can be interpreted as an attempt to sow discord, undermine trust, and potentially gather intelligence in preparation for more significant actions. The period immediately preceding the full-scale invasion on February 24, 2022, saw significant cyberattacks likely intended as a strategic distraction, potentially masking or facilitating other military preparations. In the first six months following the invasion, the main focus of cyber operations shifted towards sabotage, aiming to leak or delete critical data, thereby directly impacting the operational capabilities and information integrity of targeted entities. Subsequently, cyber tactics evolved further towards comprehensive intelligence activities, encompassing cyber, electronic, and kinetic domains. The overarching goal during this phase remained the exfiltration of vast amounts of data, suggesting an intent to gain strategic insights, identify vulnerabilities, and potentially leverage the information for future operations. More recently, a pronounced focus on the energy and finance sectors has emerged, with a significant emphasis on data exfiltration, indicating a strategic interest in disrupting critical economic functions and potentially acquiring sensitive financial information.

4.3 Best practices in cyber resilience

RQ3: What are the best practices in cyber resilience from other countries?

Addressing the multifaceted cyber threats requires a comprehensive strategy focused on building robust cyber resilience and fostering strong international cooperation:

- **Key Needs:** Ukraine requires skilled cybersecurity personnel, effective incident response mechanisms, and strong collaboration through sectoral cyber incident response centres.
- **Training and Awareness:** Emphasis is placed on training personnel in cyber hygiene through interactive platforms.

- **International Collaboration:** Ukraine actively collaborates with international partners, viewing its experience as a contribution to European security.
- **Lessons Learned:** The importance of rapid threat detection, response, data recovery, and operational continuity is paramount. Democratic nations must enhance cooperation in crisis situations.
- **Hybrid Warfare:** Recognition that cyberattacks are often part of broader hybrid operations, requiring integrated defence strategies.
- **Challenges:** The critical shortage of qualified cybersecurity personnel remains a major obstacle.
- **Mitigation:** Proactive threat monitoring, information sharing, and rapid implementation of updated security procedures are essential.

4.4 Functionality of e-services in wartime

RQ4: How has Ukraine managed to keep e-services functioning despite being an active war zone?

- Ukraine has demonstrated remarkable resilience and adaptability in the face of sophisticated cyber assaults.

- Ukraine has successfully migrated critical and sensitive data to cloud services located outside its borders.

- Ukraine has received crucial cyber and cloud services from tech giants.

- The Ukrainian case study highlights the importance of striking a balance between adaptability and strategic planning in maintaining e-services.

Interviews conducted with relevant stakeholders provide valuable insights into Ukraine's cyber warfare landscape:

- **Targeted Attacks:** Ukraine is experiencing a significant increase in cyber intrusions, particularly DDoS attacks targeting critical infrastructure like transport and energy sectors. These malicious activities are attributed to both hacktivist collectives and state-sponsored actors with suspected Russian affiliation.

- **Evolving Threats:** The nature of attacks has shifted since the full-scale invasion. Initial efforts concentrated on disseminating propaganda through media and telecommunications platforms. Current attacks exhibit a strategic shift towards the disruption of essential public services, such as energy provision and heating, with the apparent objective of societal destabilization and the infliction of human suffering.
- **Attack Patterns:** While direct attribution is difficult, Russian cybercriminals are identified as primary actors. Observed attacks encompass both high-visibility disruptive actions, likely intended for psychological impact, and clandestine espionage campaigns, exemplified by groups targeting high-ranking government officials.
- **Vulnerabilities:** Phishing remains a primary attack vector. However, a growing trend involves the exploitation of security weaknesses within third-party service providers that underpin critical infrastructure operations.
- **Impact:** The consequences of these cyberattacks extend beyond mere economic losses and service interruptions. They pose a tangible threat to national security, with potentially fatal outcomes, particularly during periods of adverse weather conditions.
- **Key Vulnerable Sectors:** Civil infrastructure, specifically the energy and transportation sector, remains acutely vulnerable due to its strategic significance for national functionality and resilience.

Long-Term Implications: Sustained cyberattacks necessitate robust cybersecurity solutions across all critical sectors to ensure long-term stability.

4.5 Observed Shifts and Emerging Trends in Cyber Warfare Tactics

Analysis of the cyberattacks against Ukraine reveals a clear temporal shift in tactics and objectives. Initially, the cyberattacks were more about causing disruption – messing things up, deleting data. There has been a discernible transition from primarily disruptive attacks, characterized by sabotage and data deletion in the initial phase of the full-scale invasion, to more intelligence-focused operations aimed at systematic data theft in the subsequent periods. This evolution suggests an adaptation of cyber strategies in response to the changing dynamics of the conflict and the strategic goals of the aggressor. Notably, the frequency and intensity of attacks have remained consistently high, demonstrating the persistent and adaptive nature of cyber threats in a protracted conflict. These attacks have continuously adapted to the evolving geopolitical situation, indicating a dynamic and responsive adversary.

5 Summary

The war in Ukraine extends beyond physical combat – it's a hybrid war with a significant cyberwarfare component. While the physical battles understandably dominate news coverage, the cyberwarfare aspect shouldn't be overlooked. Safety and cybersecurity incidents in the region have been reported for years, suggesting pre-existing conflicts that may have contributed to the current situation. The war in Ukraine highlights the increasing integration of cyberwarfare into modern conflicts and the importance of considering its impact alongside traditional military operations.

The war in Ukraine serves as a stark reminder of the importance of robust cyber defences. While Ukraine's prior focus on collaboration seems to have been beneficial, the current situation demands continuous adaptation, international support, and a focus on ensuring third-party compliance. The outcome of this cyber war will have far-reaching implications for the future of cyber security strategy around the world.

The digital age has fostered an environment where cybersecurity is no longer a luxury, but an essential element of safeguarding both individual and organizational well-being. Threat actors, encompassing criminal groups and state-sponsored entities alike, often prioritize exploiting vulnerabilities in the path of least resistance (Stallings & Brown, 2018). Whether pursuing a broad campaign or a targeted attack, adversaries will seek the most efficient means of intrusion. Consequently, every effort invested in bolstering cybersecurity posture contributes significantly to building resilience against cyber threats.

Cyber threats pose a complex and evolving challenge for governments and organizations worldwide. Decision-makers at all levels play a critical role in ensuring effective response and recovery capabilities. This section explores the importance of cyber exercises in fostering preparedness for the anticipated and unanticipated effects of cyberattacks.

The long-term implication of sustained cyberattacks could significantly hinder Ukraine's development and stability by disrupting essential services, undermining trust in digital infrastructure, and causing economic losses. The need to constantly defend against a larger aggressor also strains resources.

Another key takeaway is the value of international collaboration. Ukraine's partnership with external organizations for real-time monitoring highlights the effectiveness of a unified front against cyber threats. The Ukrainian case study offers a compelling argument for proactive cyber defence strategies. While replicating their exact approach might require adjustments, the underlying principles hold significant value for nations facing potential cyberattacks. By prioritizing data security, fostering cyber awareness, and fostering international cooperation, countries can significantly enhance their resilience in the ever-evolving digital landscape.

6 Future Work

The ongoing conflict in Ukraine presents an unparalleled opportunity for in-depth academic inquiry into the multifaceted nature of contemporary cyber warfare. Moving beyond descriptive accounts, rigorous scholarly investigation can dissect the intricate interplay of cyber operations within a broader hybrid conflict, yielding critical insights for cybersecurity theory, policy, and practice.

Key research areas:

- **Comparative Cybersecurity Resilience Across Critical Infrastructure:** This involves comparing the cybersecurity maturity, threat landscapes, third-party risk management, incident response capabilities, and service continuity across different critical infrastructure sectors in Ukraine.

- **Facilitating Global Cybersecurity Knowledge Exchange:** It focuses on identifying key lessons learned from Ukraine's wartime cyber defence, developing frameworks for international knowledge sharing and capacity building, analysing public-private partnerships, standardizing threat intelligence sharing, and exploring the ethical and legal implications of this exchange

- **The Role of State Authorities in Cyber Defence:** It analyses the strategic implementation of national cybersecurity policy, inter-agency coordination, the legal and regulatory landscape, international cooperation from a governmental perspective, and resource allocation for cyber defence.

These research avenues aim to move beyond descriptive accounts and provide rigorous academic analysis of the cyber aspects of the war in Ukraine. The findings can contribute significantly to cybersecurity theory, policy, and practice globally, informing more effective strategies and international collaborations to enhance cyber resilience in an increasingly complex digital landscape

References

Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, pp. 1-8. doi: 10.1109/PRISMS.2014.6970594

AlShihi, H. (2005). E-government development and adoption dilemma: Oman case study. In the 6th International WeB (Working for eBusiness) Conference, Victoria University, Melbourne, Australia.

Aviv, I., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection, 43*. https://doi.org/10.1016/j.ijcip.2023.100637

Bailes, A. J. K., Thayer, B. A., & Thorhallsson, B. (2016). Alliance theory and alliance 'Shelter': the complexities of small state alliance behaviour. *Third World Thematics A TWQ Journal*, *1*(1), 9–26. https://doi.org/10.1080/23802014.2016.1189806

Bendiek, A., & Bund, J. (2023, September 25). Shifting Paradigms in Europe's Approach to Cyber Defence. *Stiftung Wissenschaft und Politik (SWP)*. Retrieved from: https://www.swpberlin.org/publikation/shifting-paradigms-in-europes-approach-to-cyber-defence

Bergengruen, V. (2024). How Tech Giants Turned Ukraine Into an AI War Lab. *TIME*. https://time.com/6691662/ai-ukraine-war-palantir/

Boulègue, M., & Lutsevych. O. (2020). Resilient Ukraine: Safeguarding Society from Russian Aggression. *The Royal Institute of International Affairs.* https://www.chathamhouse.org/sites/default/files/2020-06-09-resilient-ukraine-boulegue-lutsevych.pdf

Brady, A.-M., & Thorhallsson, B. (2021). Small States and the Turning Point in Global Politics. In A.-M. Brady & B. Thorhallsson (Eds.), *Small States and the New Security Environment* (pp. 1-11). Springer. https://doi.org/10.1007/978-3-030-51529-4

Braman, E., Vaseashta, A., & Susmann, P. (2014). *Cyber Security and Resiliency Policy Framework.* IoS press. https://www.researchgate.net/publication/266077764_Cyber_Security_and_Resiliency_Policy_Framework

Brumfield, C. (Aug 24, 2022). Russia-linked cyberattacks on Ukraine: A timeline. *CSO*. Accessed 10.01.2025 https://www.csoonline.com/article/571865/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (1st ed.). 312–319. Harvard University Press.

Burton, J. (2015). NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation. *Defence Studies 15*(4), 297–319. https://doi.org/10.1080/14702436.2015.1108108.

Bygrave, L. A. (2022). Cyber Resilience versus Cybersecurity as Legal Aspiration. In T. Jančárková, G. Visky, I. Winther (Eds.), *14th International Conference on Cyber Conflict: Keep Moving* (pp. 27-44). CCDCOE Publications. https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf

Cho, S., Ertran, A., Schauss, L., Väljataga, A. Wünsche, J. (2021). Recent Cyber Events: Considerations for Military and National Security Decision Makers. NATO CCDCOE. https://ccdcoe.org/uploads/2022/02/Report_Reflections_on_2021_A4.pdf

CISA Insights. (Jan 18, 2022). *Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats*. Accessed 16.03.2024 https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf

Collier, K. (2022). Ukraine foiled Russian cyberattack that tried to shut down energy grid. *NBC NEWS.* https://www.nbcnews.com/tech/security/ukraine-says-russiancyberattack-sought-shut-energy-grid-rcna24026

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. doi: 10.22215/timreview835

Crandall, M. (2014). Soft Security Threats and Small States: the Case of Estonia. *Defence Studies*, *14*(1), 30–55. https://doi.org/10.1080/14702436.2014.890334

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). SAGE Publications, Inc. https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

Cyber Forum Kyiv. (2024). *A decade in the trenches of cyberwarfare*. Cyber Diia: https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf

Cybersecurity Strategy of Ukraine (2021-2025). Accessed 11.01.2025 https://www.president.gov.ua/documents/4472021-40013

Dacorogna, M., & Kratz, M. (2022). Special Issue “Cyber Risk and Security”. *Risks*, *10*(6), 112. Accessed 19.10.2023. https://doi.org/10.3390/risks10060112

Davydiuk, A., & Zubok, V. (2023). Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War. In 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), NATO CCDCOE, pp. 121–139. doi: 10.23919/CyCon58705.2023.10181813

Duguin, S., & Pavlova, P. (2023). The role of cyber in the Russian war against Ukraine: its impact and the consequences for the future of armed conflict. Workshop. Brussels: European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf eGA. ELi toetus küberjulgeoleku tugevdamisele Ukrainas. Accessed 10.02.2025 https://ega.ee/et/project/eli-toetus-kuberjulgeoleku-tugevdamisele-ukrainas/

Ertan, A., Floyd, K. H., Pernik, P., & Stevens, T. (Eds.). (2020). *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* NATO CCDCOE Publications. https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

ESET. (2022). ESET Threat Report T1 2022. Accessed https://www.eset.com/int/business/resource-center/reports/eset-threatreport-t1-2022/

Estonian State Information Authority. (2024). *Cyber Security in Estonia 2024*. https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf

EU4Digital (2021). *EU4Digital Facility: Public Bi-annual Report No. 5*. Accessed 08.03.2025. https://eufordigital.eu/wp-content/uploads/2021/09/EU4Digital-Facility-Public-Bi-annual-Report-No.-5.pdf

European Commission, Directorate-General for Communications Networks, Content and Technology, (2020). *The EU's Cybersecurity Strategy for The Digital Decade*. Publications Office. Accessed 10.01.2025 https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Defence Agency. (July 11, 2023). *PESCO projects adapt and accelerate amid shifting European security landscape, EU report finds*. Accessed 09.03.2024, from: https://eda.europa.eu/news-and-events/news/2023/07/11/pesco-projects-adapt-and-accelerate-amid-shifting-european-security-landscape-eu-report-finds

European Defence Agency. (n.d.-a). Permanent Structured Cooperation (PESCO). Accessed 09.03.2024 https://eda.europa.eu/what-we-do/EU-defence-initiatives/permanent-structured-cooperation-(PESCO)

European Commision. (2022). Cyber Defence: EU boosts action against cyber threats. Accessed 10.12.2023 https://www.eeas.europa.eu/delegations/montenegro/cyber-defence-eu-boosts-actionagainst-cyber-threats_en

European Parliament. (2022). *Report on security in the Eastern Partnership area and the role of the common security and defence policy (2021/2199(INI))*. Committee on Foreign Affairs. Rapporteur: Witold Jan Waszczykowski. A9-0168/2022. Accessed 09.03.2024 https://www.europarl.europa.eu/doceo/document/A-9-2022-0168_EN.pdf lk 9)

European Union Agency for Cybersecurity. (2023). *Enhanced EU-Ukraine cooperation in Cybersecurity*. Accessed 09.03. https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity.

Fahim. S. (2023). *Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges. Information*. http://dx.doi.org/10.3390/info14090485.

Finklea, K., Christensen, M. D., Fischer, E. A., Lawrence, S. V., & Theohary, C. A. (2015). Cyber Intrusion into U.S. Office of Personnel Management: In Brief. *Congressional Research Service*. https://sgp.fas.org/crs/natsec/R44111.pdf

Gavrila, A. (2022). Ukraine's great cyberwar that did not happen. *Opinion Paper*. Accessed 10.01.2025 https://www.researchgate.net/publication/365470953_Ukraine's_great_cyberwar_that_did_not_happen

Giles, K. (2023). *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine*. Research Paper, London: Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/2023-12/2023-12-14-russian-cyber-info-warfare-giles.pdf

Grossman, T. (2023, November). Cyber Rapid Response Teams: Structure, Organization, and Use Cases. *Center for Security Studies (CSS). ETH Zürich*. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securitiesstudies/pdfs/Cyber-Reports-2023-11-Cyber-Rapid-Response-Teams.pdf

Grossman, T., Kaminska, M., Shires, J., & Smeets, M. (2023). The Cyber Dimensions of the Russia-Ukraine War. *European Cyber Conflict Research Initiative*. https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf

Guchua, A., & Zedelashvili, T. (2022). The Problem of Security Protection of Strategic Objects in the Conditions of Modern Cybersecurity. *Ukrainian Policymaker*, *11*, 61-67. https://doi.org/10.29202/up/11/5

Heale, R., Forbes, D. (2013). Understanding triangulation in research. *Evidence-Based Nursing.* https://ebn.bmj.com/content/ebnurs/16/4/98.full.pdf

Hunder, M., Landay. J, Bern. S. (2023, December 13). Ukraine's top mobile operator hit by biggest cyberattack of war so far. *Reuters*. Accessed 10.11.2024 https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/

Jhanjhi, N. Z., Shah, I. A., & Rajper, S. (2022). *Cybersecurity Measures for E-Government Frameworks. chapter Introduction XXIV*. (pp.187-222). IGI Global Scientific Publishing. doi: 10.4018/978-1-7998-9624-1

Kert-Saint Aubyn, M. (n.d.). EU Adopts Network and Information Security Directive that Sets Security Rules on National Critical Infrastructure. *NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved 09.03.2024, from: https://ccdcoe.org/incyder-articles/eu-adopts-network-and-information-security-directive-that-sets-security-rules-on-national-critical-infrastructure/

Lagvilava, L. (2023). The 2022-2023 Russia-Ukraine War and Cyberspace Threats. *Future Human Image*, *19*, 41–50. doi: 10.29202/fhi/19/6

Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*. https://www.researchgate.net/profile/James-Lewis-9/publication/245508226_Assessing_the_Risks_of_Cyber_Terrorism_Cyber_War_and_Other_Cyber_Threats/links/5e25be2192851c89c9b49515/Assessing-the-Risks-of-Cyber-Terrorism-Cyber-War-and-Other-Cyber-Threats.pdf

Lindström, L., Jančárková, T., Visky, G., & Zotz P. (Eds.). (2021). 13th International Conference on Cyber Conflict : Going viral. *NATO CCDCOE Publications*. https://ccdcoe.org/uploads/2021/05/CyCon_2021_book_Small.pdf

Ministry of Foreign Affairs of Ukraine. (Feb 9, 2024). *Kyiv hosted the first Kyiv International Cyber Resilience Forum 2024: "Resilience At The Cyberwar"*. Accessed 10.01.2025 https://mfa.gov.ua/en/news/u-kiyevi-vidbuvsya-pershij-kiyivskij-mizhnarodnij-forum-z-kiberbezpeki-2024-stijkist-pid-chas-kibervijni

Najafli, E. (2022). Digital state in the context of legal reform in Ukraine: Theoretical and legal aspect. *Pravo ì Bezpeka*, *85*(2), 202-217. https://doi.org/10.32631/pb.2022.2.19

National Security and Defense Council of Ukraine (March 4, 2021). *The working group at the NCCC at the NSDC of Ukraine approved the draft Cybersecurity Strategy of Ukraine*. Accessed 21.02.2025 https://www.rnbo.gov.ua/en/Diialnist/4838.html

National Institute of Standards and Technology. (n.d.). *Cybersecurity*. NIST Computer Security Resource Center. Accessed 10.11.2024 from https://csrc.nist.gov/glossary/term/cybersecurity

NCS Guide. (2021). The guide to developing a national cybersecurity strategy. Accessed 09.03.2024 https://ncsguide.org/the-guide/

Nehrey, M., Voronenko, I., & Salem, A.-B. M. (2022). Cybersecurity Assessment: World and Ukrainian Experience. 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, pp. 335–340. doi: 10.1109/ACIT54803.2022.9913081

Neuneck, G. (2013). Assessment of international and regional organizations and activities. In: Lewis, J.A. & Neuneck, G. The Cyber Index – International Security Trends and Realities. Geneva: UN Institute for Disarmament Research. Accessed 6.10.2024 http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Newbill, C. M. (2019). Defining Critical Infrastructure for a Global Application. *Indiana journal of global legal studies, 26*(2), 761–780. https://doi: 10.2979/indjglolegstu.26.2.0761

Microsoft Security Blog. (2016). Cybersecurity and cyber-resilience – Equally important but different. Accessed 16.03.2024 https://blogs.microsoft.com/microsoftsecure/2016/11/03/cybersecurity-and-cyber-resilience-equally-important-but-different/

O'Connor, P. (2022). Ukraine: The Cyber Battlefield. *ITNow 64(*2), 42–43. doi: 10.1093/itnow/bwac053

OECD (Oct 4, 2022). *Administrative Service Delivery during War Time*. Accessed 10.11.2024 https://doi.org/10.1787/23d5a973-en

Operational Center for Cyber Incident Response, State Cyber Protection Center, State Service of Special Communications and Information Protection of Ukraine. (2021). *Annual report on the vulnerability detection system and response to cyber incidents and cyberattacks for 2021*. Accessed 10.11.2024 https:// cert.gov.ua/files/pdf/SOC_Annual_Report_2022. pdf

Osula, A.-M., & Kaska, K. (2013). *National Cyber Security Strategy Guidelines.* NATO CCDCOE Publications. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

Petrov, S. (2021). Development of the national cybersecurity system of Ukraine as a necessary element of information society development. *Bulletin of Kharkiv National University of Internal Affairs, 95*(4), 146-156. (19.10.2023). https://doi.org/10.32631/v.2021.4.12

Pravdiuk, A. (2022). The state and current issues of legal regulation of cyber security in Ukraine. *European Political and Law Discourse, 9*(3), 19–28. http://socrates.vsau.org/repository/getfile.php/31305.pdf

Reuters. (Feb 28, 2022). Satellite outage knocks out control of Enercon wind turbines. Accessed 01.03.2025 https://www.reuters. com/business/energy/satellite-outage-knocks-outcontrol-enercon-wind-turbines-2022-02-28/

Riigi Infosüsteemi Amet (2023). *Küberturvalisuse aastaraamat*. Accessed 11.10.2024 https://www.ria.ee/media/2653/download

Riigi Infosüsteemi Amet (2024). *Küberturvalisuse aastaraamat*. Accessed 09.03.2025 https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf

Rodríguez, A. G. (2022). Lessons from the Ukrainian cyber front. *European Policy Centre*. Accessed 02.02.2025 https://www.epc.eu/en/Publications/Lessons-from-the-Ukrainian-cyber-front~476f1c

Saar, J., Sinisalu, A., Loik, R., Koort, E., Tammel, K., Savimaa, R. (2024). Venemaa võimalike arengute mõjust Eesti julgeolekule. *Sisekaitseakadeemia digiriiul*. https://doi.org/10.15158/dehc-qy92

Satter, R., & Pearson, J. (2022). Exclusive: Ukraine prepares potential move of sensitive data to another country - official. *Reuters.* https://www.reuters.com/world/europe/exclusive-ukraine-prepares-potential-move-sensitive-data-another-country-2022-03-09/

Serpanos, D., & Komninos T. (2022). The Cyberwarfare in Ukraine. *Computer, 55*(7), 88–91. doi: 10.1109/MC.2022.3170644

Shea, S., Gillis, A. S., & Clark, C. (2023). What is cybersecurity? Accessed 03.03.2024 from *Techtarget*. https://www.techtarget.com/searchsecurity/definition/cybersecurity

Smith, B. (June 2, 2022). Defending Ukraine: Early Lessons from the Cyber War. *Microsoft*. Accessed 10.01.2025 https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Stallings, W., & Brown, L. (2018). Computer security: principles and practice (4th ed.). Pearson Education Limited.

State Service of Special Communications and Information Protection of Ukraine (2024). *Russian Cyber Operations. APT Activity Report H1 2024.* Accessed 15.01.2025 https://cip.gov.ua/services/cm/api/attachment/download?id=65898

Stein, J. (2024). Ukraine is on the front lines of global cyber security. *Atlantic Council.* Accessed 15.01.2025 https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-is-on-the-front-lines-of-global-cyber-security/

Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research, 2*(2), 147-184. (19.10.2023). https://doi.org/10.1007/s41125-017-0020-x

United Nations. (2023). *Statement by the Delegation of Ukraine under agenda item "Capacity Building" of the Fourth session of the Open-Ended Working Group on the security of and in the use of ICTs (2021 - 2025)* - UN Meetings. Accessed 10.01.2025 https://estatements.unmeetings.org/estatements/12.1255/20230309150000000/rqRb0soaU5CB/61Lw4qLK531r_en.pdf

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., Orlovskyi, R. (2020). Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues, 9*(3), 775-784. https://doi.org/10.9770/jssi.2020.9.3(4)

Välisministeerium. (s.a.). *Tallinna mehhanism*. Accessed 10.03.2025 https://www.vm.ee/rahvusvaheline-oigus-ja-kuberdiplomaatia/digi-ja-kuberdiplomaatia/tallinna-mehhanism

Wagner, D. (2016). The Growing Threat of Cyberattacks on Critical Infrastructure. *IRMI.* https://www.irmi.com/articles/expert-commentary/cyberattack-criticalinfrastructure

Weiss, J., Jankauskas V. (2019). Securing cyberspace: How states design governance arrangements. *Governance*, *32*(1), 3-20. https://doi.org/10.1111/gove.12368

Whyte, C., Thrall, A. T., & Mazanec, B. M. (Eds.). (2020). *Information warfare in the age of cyber conflict* (1st ed.). Routledge.

Willett, M. (2022). The Cyber Dimension of the Russia-Ukraine War. *Survival*, *64(*5), 7–26. doi: 10.1080/00396338.2022.2126193

Williamson, G. R. (2005). Illustrating triangulation in mixed-methods nursing research. *Nurse Res, 12*(4), 7–18. DOI: 10.7748/nr2005.04.12.4.7.c5955

World Economic Forum papers. (2012). *Partnering for Cyber Resilience*. Accessed 16.03.2024http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

Zetter, K. (2022). What we know and don’t know about the cyberattacks against Ukraine - (updated). *Zero Day*. Accessed 16.03.2024 https://www.zetter-zeroday.com/what-we-know-and-dont-know-about/

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Andrea Kivi

3. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Cyber resilience in Ukraine after beginning of Russia’s full-scale invasion”, supervised by Sille Arikas
   3.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   3.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
4. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
5. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Interview Questions

1. What are the most common types of cyberattacks targeting Ukraine?
2. Have you observed any significant shifts in the nature or frequency and trends of attacks over the recent years after the beginning of the full-scale invasion?
3. Have you observed any specific attack patterns?
4. What are the primary vulnerabilities or weaknesses in Ukraine's critical infrastructure or systems that make them attractive targets for cyberattacks?
5. How have cyberattacks impacted Ukraine's economy, critical services, or national security?
6. Can you quantify the costs or damages associated with these attacks?
7. Are there any specific industries or sectors in Ukraine that are particularly vulnerable to cyberattacks? If so, what is the possible reason behind this?
8. What are the possible long-term implications of cyberattacks on Ukraine's development and stability?
9. How in your opinion can Ukraine/your organization build resilience and prepare for future cyber threats
10. What are the lessons the other countries could learn from Ukraine's experience in responding to cyberattacks and implementing a cybersecurity strategy?
11. How does Ukraine collaborate with other countries or international organizations to enhance its cybersecurity capacity building?
12. Are there any specific partnerships or initiatives in place?
13. What have been the biggest advantages and disadvantages of these programmes?
14. What are the biggest challenges or obstacles Ukraine/your organization is facing in its efforts to strengthen its cybersecurity posture?
15. How can these challenges be mitigated?

Transcripts of conducted interviews are available upon request.