Degree Program in Politics: Philosophy and Economics

Course of International Relations

Cyberspace as the Fifth Domain of Warfare: Evolution of EU-NATO Cybersecurity Frameworks and Their Impact on Critical Infrastructure Protection - A Case Study of Ukraine's Cyber Defence Against Russian Aggression

Prof. Raffaele Marchetti

PROFESSOR

Laila Casile Grande ID 104452

CANDIDATE

Dr. Martina Lucaccini

SUPERVISOR

Academic Year: 2024 - 2025

ABSTRACT

This thesis explores how the European Union and NATO have adapted their regulatory and strategic frameworks to address cybersecurity threats to critical infrastructure in the context of the Ukraine war. Framed by a personal and political reflection on technology, this thesis examines how cyberspace, while enabling global progress, has also become the *fifth domain* of conflict. The first chapter of the thesis, dedicated to the literature review, outlines the conceptual evolution of cyberspace, from its theoretical roots to its transformation into a geopolitical arena of confrontation between state actors, criminal groups, and hybrid threats. After providing a clear definition of cyber war, cyber warfare, and cyber attacks, the analysis of incidents such as the *Morris worm*, *Operation Moonlight Maze*, and *Stuxnet* illustrates the shift to cyber operations capable of real-world impact. The chapter also theoretically addresses the vulnerability of critical infrastructures (i.e., energy, transport, communication, and finance) to cyber threats, the difficulty of attribution in cyberspace, and the challenges this poses for legal and military coordination. The second chapter of the thesis analyses the EU and NATO's institutional responses, from the *NIS* and *NIS2 Directives*, the *Cybersecurity Act*, cross-border cooperation frameworks, to NATO's recognition of cyberspace as an operational domain in 2016. It emphasises the growing interdependence of civilian and military cyber governance and the need for collective resilience. Lastly, the third chapter presents an in-depth case study that examines Ukraine's evolving cyber resilience from 2014, the year of Crimea's annexation and the rupture with Russia, to 2024. Through a comparative analysis of multiple case studies, ranging from the early power grid blackouts in 2015 and 2016 to more recent operations such as the 2024 *FrostyGoop* attack, the research examines how Ukraine's cybersecurity capabilities developed in parallel with its integration into NATO and EU frameworks. The analysis finds that this integration played a decisive role in enhancing Ukraine's ability to anticipate, contain, and recover from cyber incidents, particularly through improved institutional coordination, legal alignment, and access to shared threat intelligence. However, persistent shortcomings remain (e.g., local networks' vulnerability, the lack of continuous staff training, and incomplete harmonisation of security standards). Cyberspace today represents the peak of tension between control and openness, transparency and opacity, innovation and destruction. Within this dichotomy, as war seeps into circuits and servers, it is critical to protect what is invisible but essential: the networks that keep us connected.

Table of Contents

INTRODUCTION

"Technology is a useful servant but a dangerous master".

— Christian Lous Lange, Nobel Lecture, 1921

The far-sighted and uneasy vision of Christian Lous Lange, Norwegian politician and Nobel Peace Prize laureate in 1921, still resonates with striking relevance today, despite the many years that have passed since his warning in 1930. Technology, now the lifeblood of social progress, has become an essential tool for nations, a means to refine strategies, accelerate timelines, and maintain a constant competitive edge. In its most revolutionary form, through the creation of the internet, it reveals its full innovative power: an energy capable of breaking down borders and dissolving distances, connecting billions of people in an instant and making the swift exchange of ideas, news, and knowledge possible. An invisible yet powerful weave that binds the world in a net of possibilities. But every network, no matter how sophisticated, carries its own knots: structural fragilities, hidden vulnerabilities, shadowy zones where invisible actors move, armed not with rifles but with code, algorithms, and intent.

It is from these gray areas, these cracks in the surface of progress, that my desire arose to interrogate cyberspace not only as a technical environment, but as a political horizon, a theatre of conflict, a space of power and resistance.

The world of technology has undergone an extraordinary journey, starting from the first experiments in the 1960s to becoming the engine of innovation and progress we know today. This evolution has brought with it opportunities that would have been unimaginable just a few decades ago, revolutionizing the way we live, work, and communicate. However, this exponential growth has also opened new frontiers to cyber threats, which have evolved in parallel with technological advancements.

In this thesis, I will retrace the main stages in the evolution of cyber threats, from the first viruses to cyber warfare attacks, focusing on the concrete realization that this so-called "virtual" world is not, in fact, parallel, it interacts with lived reality more than the human hand ever could. Its "virtual" nature, if anything, aggravates global risks, which have surpassed the traditional concept of war as we once knew it: men against men, or at most, the threat of nuclear weapons.

Today, war has shifted into the realm of Hybrid Warfare, where pressing a single key on a computer could cause more deaths and destruction than we might imagine.

The journey into the world of cybersecurity begins with Arpanet, the pioneering network developed in the 1960s, considered the "mother" of modern networks. This inter-computer connection paved the way for the global connectivity we now take for granted.

During the 1970s and 1980s, as networks developed, the first cyber threats emerged. At that time, hackers, though the term was not yet widely used, began to explore vulnerabilities in emerging systems. One of the first “viruses” to gain attention was the Creeper worm, which in 1971 appeared on screens with a message saying: *"I’m the creeper, catch me if you can!"* It wasn’t harmful, but it was a major warning sign: it showed that accessing systems and challenging their security was possible.

The 1980s saw the appearance of increasingly sophisticated viruses and malware. One of the first large-scale viruses was Brain, which appeared in 1986 and was created by brothers Basit and Amjad Farooq Alvi. Originally designed to "teach a lesson" to customers distributing pirated copies of their software, Brain demonstrated how vulnerable systems were and how impactful cyberattacks could be on everyday work.

The spread of the Internet in the 1990s brought with it a wave of new, more sophisticated threats. As digital infrastructures expanded, so did the range and impact of cyberattacks. The first attacks included worms, trojans, and DDoS attacks, which caused increasingly significant damage.

In 1999, the Melissa worm spread through Microsoft Word documents, becoming one of the first forms of phishing: it accessed Outlook and sent malicious emails to all found contacts, creating a domino effect.

The new millennium brought even greater challenges. In 2000, the I LOVE YOU worm spread rapidly via email, causing damage estimated in the billions of dollars. These events underscored the urgent need for more rigorous and innovative security measures.

These developments pushed me to reflect more deeply, not just on how cyberattacks work, but on what they reveal. I began to ask myself: how is sovereignty redefined in a world where borders are drawn not on land, but through undersea cables? What does it mean to defend a country when the attack arrives through a malicious email or a hidden backdoor in a software update? These questions, silent but insistent, shaped not only the direction of this research but the very lens through which I approached the study of digital warfare.

The 2010s marked a true turning point in the world of cybersecurity. Hackers refined their techniques, becoming increasingly sophisticated and dangerous. During this period, ransomware began to spread, malware that encrypts victims' data and demands ransom to unlock them.

A notable example is the 2016 attack on DYN, one of the largest DNS service providers, which caused widespread outages of websites and online services, proving how vulnerable critical infrastructures are.

In 2017, the WannaCry ransomware hit organizations worldwide, exploiting a Windows vulnerability. This attack paralysed hospitals, companies, and public institutions, highlighting the importance of keeping systems updated and investing in security.

Attacks like SolarWinds in 2020 revealed how even government agencies and major companies are vulnerable to advanced cyber-espionage operations. These targeted attacks, often orchestrated by state-sponsored groups, aim to steal sensitive data and sabotage strategic infrastructures.

Today, cyber threats are a constant concern, with hacker groups operating like actual companies, tailoring attacks to political, financial, or strategic targets. Digital warfare is intensifying, and cyberspace is becoming a new global battlefield.

In recent years, Artificial Intelligence (AI) has begun to play a crucial role in the field of cybersecurity. On one hand, AI is used to strengthen defences, but on the other, hackers exploit it to create even more advanced and difficult-to-detect attacks.

Attackers use machine learning algorithms to analyse vast amounts of data and behaviour, personalizing attacks far more precisely than in the past. Evolved malware, such as intelligent ransomware, can dynamically adapt to network environments, bypass traditional defence systems, and tailor ransom demands based on the value of the compromised data.

This evolution makes the fight against cyber threats even more complex, requiring increasingly advanced tools and strategies. What emerges is not just a more dangerous cyberspace, but a new dimension of conflict altogether: digital war as a geopolitical reality.

Cyberspace has now become a new battleground for nations and hacker groups. Cyberattacks are used as tools of war to undermine national security, sabotage critical infrastructures, or spread disinformation.

In the past two years, we have witnessed attacks on the strategic infrastructures of various countries, showing how hackers can directly influence the stability of entire nations. These

attacks aim to destabilize, spy, or gain strategic advantages, and are often carried out by state-sponsored groups or international criminal organizations.

Writing this thesis has meant adopting not only a critical perspective but also a passionate one. It has been a path of study and awareness, an attempt to read not only the documents and institutional reports, but also to read between the lines, to catch the silences and ambiguities in a language, security, that often hides more than it reveals.

This thesis does not, and cannot, provide solutions, because offering a solution today would imply the presumptuous belief that one could put an "end" to technological evolution. However, what has been useful to crystallize is a current snapshot of that evolution, considering that, paradoxically, something potentially useful and generally life-enhancing for humankind (and in many respects it is) could also become the source of its total destruction.

Perhaps now more than ever, the boundless ego of the human being, domineering and absolutist, is threatening the survival of humanity itself.

This work, not without difficulty even in simply finding sources truly intrinsic to the subject of cybersecurity and cyberattacks, seeks to demonstrate how much vulnerability exists in a world we label as "secure," using the case study of so-called "Critical Infrastructures." Cyberspace, today, is the mirror of our time. In that mirror, I have chosen to look with vigilant eyes and an open mind.

This thesis is the result of a personal and academic journey that has combined study, curiosity, and critical thinking. I hope that it conveys not only the complexity of the phenomenon, but also the maturation of a rigorous method of inquiry, one aimed at understanding the present in order to transform it.

CHAPTER I

Cyberspace: The *Fifth Domain* and the Frailty of Critical Infrastructures

1. Introduction

The following chapter of this thesis will be structured as follows: first, it will introduce the concept of cyberspace, tracing its origins and defining its role in modern society. Initially a theoretical construct rooted in science fiction, cyberspace has evolved into a fundamental domain influencing technological, economic, and geopolitical landscapes. Understanding its etymological and intellectual foundations explains how it has transitioned from an abstract idea to a critical sphere shaping global interactions. Building upon this foundation, the chapter explores cyberspace as the "fifth domain" of warfare. The increasing interest of both state and non-state actors in cyber capabilities underscores its strategic importance. The discussion highlights how society's growing dependence on digital networks has introduced inherent vulnerabilities, transforming cyberspace into a contested arena with significant implications for national security. Delving deeper into the landscape of cyber warfare, the chapter differentiates between cyber war and cyber warfare, clarifying their nuances and operational dynamics. The discussion includes historical examples of cyber incidents to illustrate how cyber operations unfold in both offensive and defensive contexts. These case studies highlight the evolving nature of cyber tactics and the ongoing challenges in distinguishing between cyber attacks, cyber espionage, and conventional military engagements. The chapter then shifts focus to the various cyber threat actors operating within this domain. State-sponsored groups, hacktivists, and cybercriminal organisations are analysed, with particular attention to their motivations, capabilities, and degrees of sophistication. Understanding these actors is essential to comprehending the broader cyber threat landscape and its implications for global security. Following this, the discussion moves to cyber weapons, examining their distinctive characteristics, methods of deployment, and the ethical and legal dilemmas they present. The fluid nature of cyber operations makes attribution difficult, further complicating efforts to regulate and mitigate cyber threats. Closely linked to this analysis is an exploration of different types of cyber activities, including cyber exploitation, cyber espionage, and cyber attacks. By investigating their operational methodologies and objectives, this section underscores the

challenges of defining and responding to cyber incidents. Attention then turns to critical infrastructures and their vulnerabilities in an increasingly cyber-dependent world. Essential services such as energy, transportation, and financial systems are particularly susceptible to cyber threats, with potentially severe consequences for national security and economic stability. The growing frequency and sophistication of cyber attacks targeting these infrastructures highlight the urgent need for enhanced protective measures. To illustrate the gravity of these threats, the chapter provides an in-depth discussion of real-world cyber attacks on critical infrastructures. By examining attacker methodologies and their broader implications, this section emphasises the pressing need for proactive defence mechanisms and coordinated international responses.

This chapter tries to provide a comprehensive look at cyberspace as both an enabler and a challenge in modern security. It lays the groundwork for chapter 2, which will explore the regulatory frameworks and international efforts to address the growing risks posed by cyber threats on critical infrastructures.

1.1. The History of Cyberspace - Origin and Definition

The concept of cyberspace, initially rooted in science fiction, has evolved into one of the most significant constructs of the modern technological and geopolitical landscape. The Canadian writer William Gibson coined the term "cyberspace" in his 1982 short story *Burning Chrome*[1], which was published in the journal Omni[2] and later popularised in his 1984 novel *Neuromancer*[3]. Gibson has described *Cyberspace* as:

> *"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children learning mathematical concepts [...]A graphic representation of abstract data from the databases of every computer in the human system. Unthinkable complexity. Lines of light aligned in the non-space of the mind, clusters, and constellations of data. Like city lights, receding[...]"* [4]

[1] Treccani enciclopedia: Cyber Spazio - Lessico del XXI secolo

[2] A science fiction and science magazine published in the United States and Great Britain, containing articles about scientific facts and short science fiction stories.

[3] Treccani enciclopedia: Cyber Spazio – Lessico del XXI secolo

[4] Gibson W. (1984) Neuromancer, Ace Pub., New York.

This vivid depiction of a *"consensual hallucination"* experienced daily by billions within a matrix of interconnected data systems laid the groundwork for the widespread adoption of the term *"Cyberspace"* as a domain where virtual and physical systems converge, enabling unusual interactions, communications, and information exchange. As the internet expanded, this abstract notion evolved into a core concept representing the digital infrastructure, protocols, and socio-technical interactions defining modern life.

While Gibson's work brought the term *"Cyberspace"* into popular culture, its intellectual roots extend further back. The etymological origin of the term cyberspace is older and traces back to the philosophical tradition of Classical Athens. It combines *"Cybernetics"*, derived from the Greek *"kybernetikos",* meaning "Good at steering", and "Space"[5], highlighting its basis in systems of control and communication. Additionally, this resonates with Plato's allegory of the cave, a timeless exploration of human perception and the distinction between appearances and truth; just as the prisoners in the cave perceive shadows as reality, individuals in cyberspace engage within a digitally constructed realm that both reveals and obscures the deeper structures shaping their experiences[6]. The synthesis of these ideas positions cyberspace as a modern reflection of ancient philosophical concerns, an environment simultaneously shaped by governance and human perception, where reality is mediated through control systems.

These philosophical underpinnings found a modern parallel with the advent of the Internet in the 1990s when the term took on a meaning closer to what we associate with it today: a virtual space where communication occurs through computer networks. Norbert Wiener introduced the word "cybernetics" in his seminal work *Cybernetics: Or Control and Communication in the Animal and the Machine*[7] published in 1948. Defined as the science of communication and automatic control in machines and living organisms, Wiener's ideas laid the groundwork for understanding systems of control and feedback, which later became integral to cyberspace. Moreover, the mathematical and physical notion of "space" further shapes the term, particularly the idea of topological and metric spaces from geometry and computer science[8].

[5] Encyclopedia Britannica: cybernetics

[6] Johri S. (2023) Plato’s parasocial parable of the cave. The Michigan Daily

[7] Wiener N. (1948) Cybernetics: Or Control and Communication in the Animal and the Machine, The M.I.T. Press, Cambridge, Massachusetts.

[8] Barth T. H. (2024) Cyberspace and Space Similarities, Differences, and Related National Security Issues. Institute for Defence Analyses.

Wiener's contributions extended beyond scientific theory, influencing how humanity interacts with machines and technology. Though not directly tied to modern devices, his work on feedback systems and control mechanisms influenced subsequent technological developments. The emergence of devices like tablets, smartphones, laptops, and wearables has transformed daily life, altering relationships between individuals and reshaping the dynamics between citizens and the state, as well as the world of work and the economy. This evolution has created a societal model in which information plays a strategic role. The "Information society," with its profound economic, social, political, and cultural implications, serves as a foundation for further transformation into a knowledge-based society.

The popularisation of the notion of cyberspace owes much to writer and journalist Bruce Sterling**,** who credited John Perry Barlow with describing the *"present-day nexus of computer and telecommunications networks"* [9]. In June 1990, while announcing the formation of the Electronic Frontier Foundation (EFF), Barlow described in his essay the term as follows:

> *"In this silent world, all conversation is typed. To enter it, one forsakes both body and place and becomes a thing of words alone. You can see what your neighbours are saying (or recently said) but not what either they or their physical surroundings look like. Town meetings are continuous, and discussions rage on everything from sexual kinks to depreciation schedules. Whether by one telephonic tendril or millions, they are all connected to one another. Collectively, they form what their inhabitants call the Net. It extends across that immense region of electron states, microwaves, magnetic fields, light pulses, and thought which sci-fi writer William Gibson named Cyberspace."* [10]

This description vividly captures cyberspace's abstract and disembodied nature, emphasising its function as a virtual city where words dominate interactions rather than physical presence. Sterling's and Barlow's contributions cemented the term's connection to the emerging internet culture and its role as a metaphorical space of communication and exchange. This notion illustrates how cybernetics and the broader technological world transcend physical objects or tangible elements, unveiling an invisible domain where virtual encounters take shape.

[9] Barlow's, J. P. (1996). Declaration of independence for cyberspace.
[10] Barlow's, J. P. (1990). Crime and Puzzlement.

Modern definitions of cyberspace have further refined its scope and significance. In 2008, the United States Department of Defence (DoD), headquartered at the Pentagon, convened a group of experts to establish a unified definition of cyberspace[11]. On that occasion, the DoD provided the following definition, included in its Dictionary of Military and Associated Terms:

> *"A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."* [12]

This definition captures the multifaceted nature of cyberspace, blending physical components (i.e. servers, cables, and embedded processors) with logical constructs, including software, protocols, and data. Furthermore, the socio-technical dimension of cyberspace emphasises its role as a shared space influenced by human behaviour, institutional frameworks, and cultural dynamics. Similarly, the Russian-American Cyber Security Summit defines cyberspace's hybrid nature as: *"an electronic medium through which information is created, transmitted, received, stored, processed, and deleted"* [13]. This highlights its dual nature as a technological and human construct.

Scholars have also explored this hybrid nature. For instance, Krippendorff (2009)[14] argues, "*Cyberspace results from the human collective ability to articulate possibilities in which technological artefacts are designed, used, and conceptualised"* [15]. This perspective underscores the iterative and creative processes through which humans shape cyberspace, infusing it with meaning and functionality. On the other hand, in 1984, William Gibson reiterated its definition of cyberspace on an anthropological level and described cyberspace as *"an iceberg of social change, approaching a postindustrial culture"* [16]. This metaphor highlights the profound, often unseen shifts in societal structures and human behaviour brought about by digital connectivity.

---

[11] Giovanni Campanale (2020). Dal concetto di cyber attack al cyberwarfare: l'uso della forza in ambito cyber. Article published on "Cybersecurity360".
[12] U.S. Department of Defence (2021, November). DOD Dictionary of Military and Associated Terms
[13] The Russia-U.S. Bilateral on Cybersecurity (2014) – Critical Terminology Foundations, Issue 2
[14] Krippendorff K. (2009). On Communicating, Otherness, Meaning, and Information. Fernando Bermejo (Ed.). New York, Routledge.
[15] Mbanaso U. - Dandaura E.S. (2015) The Cyberspace: Redefining A New World. Article published on IOSR Journal of Computer Engineering (IOSR-JCE)
[16] *Ibidem*.

Cyberspace catalyses new cultural behaviours, such as virtual communication, digital collaboration, and the creation of online identities, fundamentally reshaping how individuals and communities interact. By integrating institutional, technological, and cultural perspectives, cyberspace emerges as a domain of technical infrastructure and a dynamic space of human activity and societal transformation. It encapsulates the interplay between physical systems, logical constructs, and socio-cultural influences, positioning itself as a cornerstone of the modern digital age.

1.2. From Strategic Interest to the Fifth Domain of Warfare

Major powers are increasingly interested in cyberspace because its emergence has profoundly reshaped society, influencing individuals, organisations, and states alike while redistributing power in unprecedented ways[17]. Cyberspace has three defining features: youthfulness, modernity, and self-organisation.

It is considered young because the *World Wide Web,* one of the most transformative internet services, was launched on August 6th, 1991, revolutionising information retrieval through its Client-Server network model. Cyberspace is modern due to its capacity for continuous evolution, enabling rapid adaptation to technological and societal changes within seconds. Finally, it is self-organising, as its decentralised structure allows it to respond to modifications autonomously, enabling emergent patterns of order without centralised control[18]. This era has been described using various terms, such as the information age, the internet age, or the computer age, reflecting the central role of digital technologies in defining contemporary society. Cyberspace's unparalleled ability to enable instantaneous access and dissemination of information across any distance has become one of its most significant assets. The transformative potential of information lies not merely in its content but in the speed and scale at which it can be transmitted, transcending geographical borders and temporal barriers. The global shift from reliance on physical media to digital systems initially captured the attention of major global superpowers, particularly the United States, which led to efforts to harness the strategic

[17] Martino L. (2016). Between International Politics and Technology: Dominating Cyber to Control Space. Article published on "ISP" Online.

[18] Harries, D. (2017). Narrative Mapping of Cyberspace. Context and Consequences. In J. Martín Ramírez Luis & A. García-Segura (Cur.), Cyberspace Risks and Benefits for Society, Security and Development (pp. 23-40). Berlino: Springer.

opportunities offered by cyberspace. Over time, smaller states followed, recognising that this frontier provided innovative means to achieve their objectives.[19]

Integrating digital technologies into critical infrastructure, such as energy systems, transport networks, and communication frameworks, has brought considerable advantages, including improved efficiency and economic growth. However, this dependence on digital systems also introduces vulnerabilities that malicious actors can exploit, underscoring the necessity of robust cybersecurity measures. While cyberspace promises social progress, it is often weaponized to secure strategic and geopolitical advantages. Its ability to dissolve physical boundaries has compelled states to adopt new defensive and offensive strategies.

The interconnected nature of this domain, encompassing public institutions, private entities, and individual actors, has created a highly intricate landscape marked by challenges that demand innovative solutions. Both state and non-state actors play pivotal roles within this borderless realm, broadening the spectrum of potential threats and opportunities. Historically, technological development was primarily viewed as a tool for enhancing the quality of life; however, cyber tools are increasingly weaponized to target states or non-state entities[20]. This dual-use nature of technology reflects technological advancements and a profound shift in how warfare and security are conceptualised, starting a new era of conflict and geopolitical strategy.

Building on this, cyberspace has evolved from a theoretical construct into a critical domain. In 2010, William J. Lynn III, the former U.S. Deputy Secretary of Defence, notably described cyberspace as the *"fifth domain of conflict, alongside land, sea, air, and space"*[21]. This acknowledgement represents a fundamental shift in how governments and organisations approach national security, as cyber threats extend beyond the virtual world to exert devastating effects in the physical realm.

Recognising cyberspace as the *"fifth operational domain"*[22] underscores its centrality in contemporary geopolitics and critical role in enabling and coordinating military operations. However, unlike traditional domains, cyberspace is a fully human-created environment characterised by constant evolution and intangibility. Its boundaries are not physical but are

---

[19] Li, Tony Yuan. "Asymmetry in the Digital Age: Cyber Deterrence Strategies for Small States." Journal of Strategic Security 17, no. 4 (2024) : 71-88. Available at: https://digitalcommons.usf.edu/jss/vol17/iss4/5

[20] Xiangsui W. - Liang W. (2001). Unrestricted Warfare. China's Master Plan to Destroy America. Pan American Publishing Company, Panama

[21] Garamone J. (2010). Lynn Notes Cyber Command's Significance. American Forces Press Service

[22] Royal Air Force (2023). Air and Space Power Review, Vol. 18, Issue 1. Article Published on Centre for Air and Space Power Studies.

defined by networks, data flows, and technological innovations. This unique nature introduces complexities in governance and defence, as control over cyberspace is inherently fragmented, limited to specific networks, and resistant to comprehensive domination.[23]

The creation of the U.S. Cyber Command exemplifies the increasing militarisation of cyberspace. Its primary objectives include protecting critical infrastructure, preserving operational freedom, and denying adversaries access. Military strategists increasingly view cyberspace as integral to multi-domain operations (MDO)[24], which synchronise actions across land, sea, air, space, and cyberspace to achieve strategic objectives. This integrated approach acknowledges the interdependence of domains, with cyberspace serving as a critical enabler for intelligence, surveillance, precision strikes, and operational coordination.

From a technical perspective, cyberspace operates through interactions within distributed systems comprising[25]: *(i)* Locations (i.e. physical and virtual points where resources and processes reside); *(ii)* Resources (i.e. elements such as computational power, data storage, and human inputs); *(iii)* Processes (i.e. activities and operations that facilitate data transmission, computation, and user interaction). The fifth domain of warfare stems from the dual identity of cyberspace as both a realm of opportunity and a source of vulnerability. It fosters global connectivity, drives economic growth, and accelerates innovation. Cyberspace enables the digital economy, supports governance, and enhances societal interactions. Technologies such as cloud computing, the Internet of Things (IoT)[26], and artificial intelligence exemplify how cyberspace reshapes industries and daily life. However, it is also inherently susceptible to risks, including cyberattacks, espionage, and the exploitation of critical infrastructure; the interconnected nature of cyberspace amplifies these vulnerabilities, as adversaries can exploit weak points to disrupt networks, steal sensitive information, or sabotage critical systems.

Cyberspace's strategic importance is heightened by its central role in the global information economy, where governments, businesses, and individuals depend on it for productivity, innovation, and governance. However, this reliance also creates a digital divide between nations

[23] Martino L. (2018). The Fifth Dimension of Conflictuality: The Rise of Cyberspace and Its Effects on International Politics.
[24] NATO Allied Command Transformation (2023). MDO in NATO Explained.
[25] Collinson M. -Monahan B. - Pym D. (2012). A Discipline of Mathematical Systems Modelling. London: College Publications.
[26] The Internet of Things (IoT) refers to physical objects embedded with sensors that communicate with computers. The IoT enables the physical world to be digitally monitored or controlled.

with advanced technological capabilities and those struggling to adapt[27]. Countries compete for dominance in cyberspace as they leverage technological innovation to assert geopolitical influence**.** This rivalry is particularly apparent in the cybersecurity industry, where nations invest heavily in protecting their networks while developing offensive capabilities[28].

As cyberspace continues to evolve, its integration into multi-domain operations underscores its indispensable role in modern warfare. NATO and allied forces emphasise the importance of incorporating cyberspace into their strategic frameworks, recognising its potential to enhance operational effectiveness across all domains. However, militarising cyberspace raises ethical and legal questions, particularly regarding using offensive cyber capabilities and protecting civilian infrastructure.[29]

Once a fictional concept, cyberspace is now an essential domain for human activity and military strategy, reflecting its profound impact on modern society. Its recognition as the fifth domain of warfare underscores its importance in shaping the future of geopolitics, security, and societal development.[30]

1.3. The notions of Cyber War and Cyber Warfare through Early Cyber Attacks

Before providing an overview of the concept of cyber war and cyber warfare, it is essential first to assess what war itself entails. The fundamental characteristics of war, as articulated by Prussian General Carl von Clausewitz, continue to underpin much of contemporary thinking about conflict. Clausewitz famously defined war as: *"nothing but a duel on a larger scale"*[31], a physical contest between adversaries, each employing *"force to compel our enemy to do our will"*. He asserted that *"there is only one means in war: combat"*[32], emphasising that at its core, *"war is fighting"*[33]. The defining element of war, according to Clausewitz, is the spilling of blood, which makes *"it a special activity, different and separate from any other pursued by man"*[34].

[27] Moschetta G. - Winslow E. (2025) Geopolitical tensions, AI and more are complicating the cyberspace. Here's what to know. World Economic Forum.
[28] Fick N. et al. (2022) Confronting Reality in Cyberspace Foreign Policy for a Fragmented Internet. Council on Foreign Relations
[29] North Atlantic Treaty Organization (2024) Cyber Defence.
[30] *Ibidem.*
[31] Douglas O. (2024) On Cyber War. The Cove.
[32] *Ibidem.*
[33] *Ibidem.*
[34] *Ibidem.*

Although these theories were formulated nearly 185 years ago, they remain highly relevant, particularly in the context of modern warfare. The rise of non-state actors and the increasing significance of cyber operations have expanded the scope of conflict beyond traditional battlefields. Clausewitz's framework continues to provide insights, especially as warfare now extends into the digital domain. His principles remain applicable in the Computer Age, aiding in the analysis of contemporary challenges and evolving strategies in modern warfare, including cyberwar and cyber warfare.

Traditionally, wars aimed at expanding territorial control and subjugating populations, thereby increasing supremacy and hegemony. Conflicts involved physical armies engaging directly on battlefields. However, technological advancements and shifts in diplomacy have transformed methodologically and intensified the nature of warfare. This growing reliance on digital technologies has redefined how conflicts are conceptualised and executed[35].

Attention has shifted to the digital domain, where states and individuals use advanced technological tools to launch cyberattacks. In this context, the traditional notion of *"war"* must be expanded to include and differentiate between three key concepts: *"cyber attack," "cyber warfare"* and *"cyber war."* While closely related, these terms resist a unified definition and have been refined through years of dedicated study.

One of the earliest comprehensive perspectives on cyber war comes from Arquilla and Ronfeldt (1993):

> *"Cyberwar refers to conducting and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the balance of information and knowledge in one's favour, especially if the balance of forces is not. It means using knowledge so that less capital and labour may have to be expended."*[36]

[35] Dasetty A. G. - Jangampet V. D. (2023). Protecting Critical Infrastructure from Cyber Attacks: A Multifaceted Approach. IJARST

[36] Arquilla J. & Ronfeldt D. (1993). Cyberwar is coming! Santa Monica, CA: RAND Corporation

This definition highlights the strategic element of cyberwar, emphasising information control, disruption, and the advantage gained through superior knowledge rather than traditional military force.

A second definition, offered by Taddeo (2012), refines instead the notion of cyber warfare by outlining its key characteristics and objectives:

> *"The warfare grounded on certain uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances."* [37]

These definitions provide the foundation for distinguishing cyber attacks, cyber warfare, and cyber war.

A cyber attack refers to offensive or defensive cyber operations capable of causing significant harm[38]. This harm can manifest in diverse forms, from physical injuries or fatalities to damage or destruction of infrastructure, economic disruption, or psychological distress.

Conversely, cyber warfare refers to using cyberattacks with malicious intent to obtain, destroy, or alter information within a broader military strategy[39]. Lastly, cyber war is characterised by two primary conditions: the declaration of war by a nation-state and the execution of that war entirely within the cyber domain[40]. Therefore, while cyber warfare is an activity, cyber war represents an ongoing conflict.

Determining whether cyber operations constitute cyber warfare requires examining two key factors: intent and the actor involved. Intent involves assessing the purpose behind a cyber operation, such as achieving military objectives. The actor, whether a nation-state, terrorist group, or individual, is critical in establishing the connection to warfare intent. For instance, cyber activities attributed to nation-states or terrorist groups are more likely to align with warfare objectives than those conducted by independent individuals.

---

[37] Taddeo, M. (2012). An analysis for a just cyber warfare. 2012 4th International Conference on Cyber Conflict (CYCON 2012).

[38] Schmitt, M. N. (Cur.). (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press. Consulted from https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf. (p. 106).

[39] Lisi, S., - Gori, U. (2015). Cyber Warfare 2014: armi cibernetiche, sicurezza nazionale e difesa del business. Cyber Warfare 2014, 1-287.

[40] Clarke, R. A.- Knake, R. K. (2014). Cyber war. Old Saybrook: Tantor Media, Incorporated.

Cyber operations can take various forms: *(i)* cyber attacks are targeted actions aimed at paralysing, disabling, or damaging the adversary's computer systems, thereby achieving the primary objectives of cyber warfare; *(ii)* information-gathering activities (i.e. Intelligence) and cyber espionage focused on collecting sensitive data; *(iii*) cyber defence**,** encompassing a range of operations designed to protect cyberspace from cyber attacks associated with a cyberwar; and *(iv)* propaganda and dissemination of messages intended to misinform citizens and weaken the enemy's morale, employing strategies typical of psychological warfare[41].

Defining cyber warfare within the traditional boundaries of conflicts between states is increasingly complex in an interconnected world. Such activities are typically conducted covertly, with unpredictable methods, and their effects often remain hidden or unclear in the immediate aftermath. Cyber warfare transcends physical borders, making it particularly challenging to identify and attribute attacks targeting states or organisations. This relates well with the concept of unrestricted warfare:

> *"When we suddenly realise that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form of war: Warfare which transcends all boundaries and limits, in short: unrestricted warfare."* [42]

These are the words of two Chinese generals from the late 1990s, who argued that no apparent boundaries exist for what we now refer to as cyber warfare. They emphasised the absence of defined limits or borders that could help concretely characterise this new form of conflict. This perspective also underscores a central debate in contemporary literature: whether all the tools and methods we know can be applied in this "unrestricted warfare."

The genesis of cyberwarfare can be traced to early cyber incidents and a growing understanding of how digital systems could be weaponized for strategic purposes. The Morris Worm[43] incident in 1988 was one of the earliest large-scale demonstrations of how software could disrupt interconnected systems globally. Though unintended, this self-replicating worm revealed the fragility of computer networks and how they could be exploited; it also marked the beginning of

[41] *Ibidem*.
[42] Xiangsui W. - Liang W. (2001). Unrestricted Warfare. China's Master Plan to Destroy America. Pan American Publishing Company, Panama. p 12
[43] Federal Bureau of Investigation (2018). The Morris Worm: 30 Years Since First Major Attack on Internet. FBI News.

recognising cyberspace as a domain where adversarial actions could occur. Initially designed as an academic experiment, the worm ended up turning off approximately 10% of the Internet-connected systems of its time[44]. This event highlighted how even unintended cyber attacks could have widespread consequences.

During the 1990s, cyber incidents became more targeted and sophisticated, prompting a shift from unintentional damage to deliberate exploitation of digital systems. Operation Moonlight Maze[45], from 1996 to 1999, exemplified this evolution. This cyber-espionage campaign, believed to be state-sponsored, targeted U.S. government and military networks, resulting in the theft of large volumes of sensitive information, including classified military plans and personnel records. It was one of the first operations to demonstrate how cyberspace could be systematically used for strategic intelligence gathering, reinforcing its significance as a future battlefield. By exploiting vulnerabilities in digital infrastructure, Operation Moonlight Maze solidified the concept of cyberspace as a domain where nations could compete for power and influence without traditional kinetic warfare.

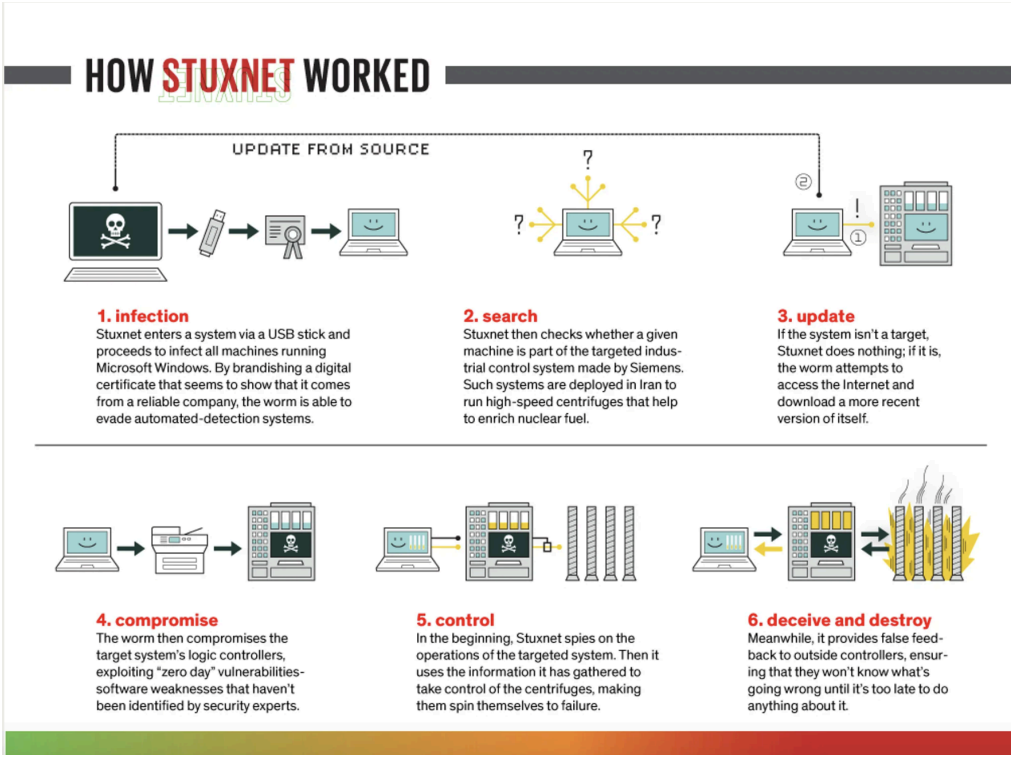
The late 1990s and early 2000s saw the formalisation of cyberwarfare as policymakers, militaries, and technologists began to view cyberspace as an extension of the traditional domains of conflict.[46] In this period, the United States and other major powers began incorporating cyber capabilities into their national defence strategies. The 1991 Gulf War, for instance, demonstrated early applications of cyber tactics when coalition forces disrupted Iraqi communications systems to gain an advantage. This was an early precursor to the deliberate and structured use of cyber operations compared to conventional military efforts[47]. By the early 2000s, concepts like "information warfare" and "network-centric warfare" gained traction, emphasising the strategic value of dominating the information space and exploiting digital networks for military advantage.

The deployment of Stuxnet in 2010 marked a watershed moment in the maturation of cyber warfare as a field. Stuxnet, often described as the first case of cyberwar, was a highly sophisticated piece of malware specifically designed to target Iran's nuclear enrichment program

[44] Paganini S. (2013). Il primo ‘worm’ su Internet non si scorda mai: era il 1988 e internet conobbe il ‘Morris Worm’. Archeologia Informatica.
[45] Comitato Atlantico Italiano (2014). *Quale approccio per una minaccia nuova?*. Intervento alla Cyber Warfare Conference, Sala dei Gruppi Parlamentari della Camera dei Deputati, Roma, 11 giugno 2014.
[46] Tepper E. (2022). The First Space-Cyber War and the Need for New Regimes and Policies. Centre for International Governance Innovation.
[47] *Ivi*, p.2.

at Natanz. Unlike earlier cyber incidents primarily focused on data theft or network disruption, Stuxnet was designed to cause physical damage. It infiltrated Siemens SCADA systems controlling uranium-enrichment centrifuges and subtly altered their operation[48]. By changing the rotational speed of the centrifuges while displaying regular readings to operators, Stuxnet caused significant physical damage to the equipment without immediate detection. The Stuxnet malware operated by targeting a closed system isolated from external access. It relied on an infected USB drive, likely used by an engineer working at the target location, as its entry point. Once introduced, the malware exploited four separate zero-day vulnerabilities to infiltrate multiple machines, ultimately reaching the SCADA devices[49]. This multi-step process was necessary because direct infection of the target system was impossible. Instead, Stuxnet leveraged vulnerabilities in intermediary devices to gradually advance toward its final objective.

Figure 1: Scheme of Stuxnet Infection[50]



Source: Kushner D. (2024). The Real Story of Stuxnet. IEEE Spectrum.

[48] Kushner D. (2024). The Real Story of Stuxnet. IEEE Spectrum.
[49] *Ibidem.*
[50] *Ibidem.*

Stuxnet represented a paradigm shift in the use of cyber tools. It demonstrated how cyberattacks could achieve strategic objectives traditionally associated with kinetic warfare without physical military intervention. Its use of multiple zero-day exploits[51] and advanced obfuscation techniques showcased the increasing sophistication of cyber operations. The operation, widely attributed to a collaboration between the United States and Israel, was part of a broader effort to delay Iran's nuclear program while avoiding the geopolitical risks associated with conventional military strikes.

The impact of Stuxnet extended far beyond its immediate target. Cybersecurity experts' discovery and reverse engineering exposed the world to the potential of cyber weapons, sparking a global arms race in cyberspace. Nations began investing heavily in offensive and defensive cyber capabilities, recognising the strategic advantages of controlling this domain. Stuxnet also highlighted the ethical and legal challenges of cyber warfare. Targeting civilian infrastructure blurs the lines between military and non-military objectives, raising questions about the applicability of international law in regulating cyber conflict.

The birth and evolution of the concept of cyber warfare have fundamentally reshaped the global security landscape. From the early incidents of the Morris Worm and Moonlight Maze to the sophisticated deployment of Stuxnet, these events have demonstrated the transformative power of cyberspace as a domain of conflict. Cyber warfare is an established reality today, influencing military doctrine, national security policies, and global power dynamics. Its significance lies in its ability to disrupt and destroy and its capacity to redefine the nature of conflict in an increasingly interconnected world.

1.4. Threat Actors: Cyber Warfare Perpetrators

In the evolving cybersecurity landscape, the term "threat actor" has become central to understanding the dynamics of modern cyber threats. According to the National Institute of Standards and Technology (NIST), a threat actor is *"an individual or group that poses a potential risk to organisational systems, operations, or data by leveraging unauthorised access or exploiting vulnerabilities"*[52]. These actors operate with diverse objectives, from disrupting services to obtaining sensitive information, and are characterised by their varying resources,

[51] A zero-day exploit is a cyberattack vector that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware. Source IBM.

[52] Johnson C. et al. (2016). Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150

expertise, and motivations. The subsequent analysis will delve into categorising threat actors and the motivations driving their actions. The main actors operating in cyberwarfare are the following: cybercriminals; hacktivists[53]; state actors; Script Kiddies[54]; crime groups; and terrorist groups.

However, it is essential to move beyond this distinction to grasp the concept entirely. We can categorise cyber actors into state and non-state groups. State actors include governments, defence ministries, and public organisations, which may rely on skilled internal personnel or collaborate with non-state operators to pursue political, military, or administrative goals. Advanced state actors such as Russia, China, Iran, and North Korea represent sophisticated threats. In contrast, non-state actors encompass independent professionals, private companies, activists, and militants. These individuals or groups engage in cyber operations for ideological or financial reasons, either working autonomously or acting on behalf of others.

Career cybercriminals constitute one of the most prevalent and financially motivated threat actors. Operating individually or as part of a network, their primary objective is exploiting vulnerabilities for monetary gain[55]. These actors frequently employ phishing, ransomware, and malware to infiltrate systems and extract valuable data. Ransomware attacks, for example, involve encrypting a victim's data and demanding a ransom in exchange for its release. Beyond ransomware, they engage in data theft, targeting sensitive information such as credit card numbers and personal identification, as well as fraud schemes designed to exploit individuals and organisations[56].

Ideological, political, or social motivations primarily drive hacktivists[57]. Unlike career cybercriminals, their objective is not financial profit but rather the pursuit of a cause or the desire to bring attention to perceived injustices. Hacktivists typically target organisations, governments, or entities they view as unethical or oppressive. Their methods include website defacements, distributed denial-of-service (DDoS) attacks, and data leaks. Prominent hacktivist groups such as

---

[53] The term “Hacktivist” derives from “Hacktivism,” meaning: “computer hacking (as by infiltration and disruption of a network or website) done to further the goals of political or social activism.” Definition from Merriam-Webster Online Dictionary, accessed January 23, 2025, https://www.merriam-webster.com.

[54] The term “Script Kiddies” refers to “a person who uses existing programming code to hack somebody's computer, because they do not have the skill to write their own code.” Definition from Oxford Advanced Learner's Online Dictionary, accessed January 23, 2025, https://www.oxfordlearnersdictionaries.com.

[55] Duffy C. (2020) Cyber attacks are increasingly all about financial gain, report says. CNN Business.

[56] Sophos (no date). What are the Types of Cyber Threat Actors?

[57] *Ibidem.*

Anonymous[58] use these tactics to challenge institutional power and promote transparency, often operating in decentralised and anonymous networks of the *Dark Web*[59] to protect their identities.

State-sponsored actors represent some of the most resourceful and advanced players in cyberwarfare. Backed by national governments, their activities include cyberespionage, which involves stealing sensitive information to gain a political, economic, or military advantage, and sabotage through deploying sophisticated cyber weapons. The Stuxnet malware, believed to have been developed by the United States and Israel, provides a clear example of state-sponsored cyber operations to undermine a nation's critical infrastructure.

Insider threats come from individuals within an organisation who exploit their access to systems and data for malicious purposes. These individuals may be employees, contractors, or business partners. Their motivations vary, ranging from personal grievances and financial incentives to coercion by external actors. Insider threats are hazardous because they can bypass external security measures, making their activities harder to detect. A notable example is Edward Snowden[60], whose unauthorised disclosures exposed extensive surveillance programs conducted by the National Security Agency (NSA)[61].

Often considered the least sophisticated threat actors, script kiddies use pre-existing tools and scripts to carry out cyberattacks without deep technical expertise. Their motivations are usually trivial, such as seeking attention, proving their abilities, or having fun. Despite their lack of sophistication, script kiddies can cause significant disruptions, mainly if they exploit unpatched vulnerabilities in widely used systems[62].

Organised crime groups incorporate cyberattacks into their broader criminal activities, often treating cyberspace as an extension of their traditional operations. These groups operate with structured hierarchies and employ specialised personnel to conduct financial fraud, identity theft,

[58] "Anonymous" is the name of an international organization of activists who act anonymously, either in coordination or individually, against all forms of censorship and misinformation, in the name of freedom of speech and human rights.

[59] The term "dark web" refers to the deepest part of the deep web, composed of so-called DarkNets: these are contents intentionally hidden from regular users and accessible only through specific anonymity tools.

[60] Edward Snowden, an American computer scientist and activist born in 1983, worked for the NSA and CIA in the field of cybersecurity. In 2013, he revealed thousands of classified documents to *The Guardian* about global mass surveillance, exposing violations of privacy and freedom of information. Accused of espionage by the United States, he was granted asylum in Russia and obtained political refugee status from the EU in 2015. Since. Source: Treccani enciclopedia

[61] The National Security Agency (NSA) protects national security systems and information. Official Website of the United States Government

[62] Sophos (no date). What are the Types of Cyber Threat Actors?

and selling illicit goods on dark web marketplaces. The integration of advanced technology allows them to evade detection and maximise profits[63].

Terrorist organisations increasingly leverage cyber capabilities to further their ideological and political objectives. Cyberterrorism enables these groups to disrupt critical infrastructure, spread propaganda, and recruit members, often amplifying their reach and impact.

To effectively prevent cyberattacks, it is crucial first to understand the motivations driving threat actors to target specific systems or data. Financial gain[64] remains one of the most prevalent motivations among cybercriminals. Threat actors seeking monetary rewards often aim to steal sensitive information, such as data that can be sold on the black market or used for fraud. This is a driving factor behind ransomware attacks, where victims are coerced into paying substantial sums to regain access to their encrypted data.

Espionage[65] is another significant driver of cyber activities. Nation-states, corporate competitors, and other entities engaged in cyber espionage to gather valuable information, including trade secrets, intellectual property, or government intelligence. These activities provide political, economic, or strategic advantages serving national interests, often involving state-sponsored actors equipped with advanced resources. For some, ideological or political motives underpin their actions. Hacktivists, for instance, target organisations or systems to promote their beliefs, raise awareness or protest perceived injustices to draw attention to their agendas. Certain threat actors aim to sabotage and disrupt critical infrastructure or operations beyond financial or ideological goals. These motivations often stem from political or ideological objectives and can lead to widespread disruptions, financial losses, and damage to public trust[66]. Political discord is another area where cyber methods are used. Extremist groups frequently use cyber tactics to disseminate propaganda, recruit members, and coordinate activities. Additionally, business competitors may use cyber activities to gain an advantage by stealing proprietary information, disrupting operations, tarnishing reputations and businesses[67]. Understanding threat actors' diverse motivations is only part of the challenge. Their capabilities, which vary depending on their resources, expertise, and objectives, also play a critical role in determining the nature and impact of cyber threats. Standard capabilities include malware development, such as

[63] *Ibidem.*
[64] *Ibidem.*
[65] *Ibidem.*
[66] Threat Actors & its Types (2025) Cyble.
[67] *Ibidem.*

ransomware, trojans, and viruses, and exploiting software vulnerabilities to infiltrate systems. Threat actors may also employ website defacement, DDoS attacks, and data breaches to disrupt operations or expose sensitive information.

More advanced actors, particularly state-sponsored groups, possess sophisticated tools and techniques that enable long-term infiltration, data exfiltration, and advanced persistent threats (APTs). These actors often deploy zero-day exploits, conduct supply chain attacks, and develop advanced cyber weapons. They also engage in prolonged espionage campaigns to achieve geopolitical or strategic objectives.

As technology evolves, so do the methods and capabilities of threat actors. Emerging tools and techniques continue to reshape the cyber threat landscape, underscoring the importance of vigilance and robust cybersecurity measures for organisations and governments.

1.5. Cyber Weapons in Cyber Warfare

The concept of cyber weapons has a central role in cyber warfare. Therefore, it is necessary to understand their nature, application, and implications clearly. Cyber weapons differ fundamentally from ordinary hacker attacks due to their complexity, purpose, and strategic use in military or intelligence operations.

Cyber weapons are sophisticated tools, often consisting of intricate lines of code, explicitly designed to achieve strategic objectives in the digital domain. In their seminal work published in 2012, Rid and McBurney provide an essential perspective, defining cyber weapons as: *"non-physical instruments created to disrupt, degrade, or manipulate adversary digital systems, typically in contexts involving military or strategic competition"* [68]. Unlike generic cyberattacks, these tools are designed with precision and intent, targeting critical vulnerabilities to maximise their impact.

To fully delineate a cyber weapon, three critical characteristics must be considered.[69] First, the context. Cyber weapons are typically employed within a defined conflict framework involving state or non-state actors. They operate as tools in broader cyber warfare campaigns or geopolitical disputes. Secondly, another essential element is the purpose; the primary aim of cyber weapons is to inflict tangible damage, whether by causing physical destruction to

[68] Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, *157*(1), 6–13. https://doi.org/10.1080/03071847.2012.664354

[69] S. MELE, "Cyber-Weapons: aspetti giuridici e strategici", op. cit., p. 10

infrastructure or compromising the operational capacity of information systems. Such damage may include disabling critical infrastructure, stealing sensitive data, or spreading disinformation to destabilise a nation. Finally, we should consider the relevance of means: cyber weapons require specific platforms, such as custom software or hardware, that exploit system vulnerabilities or leverage advanced techniques like zero-day exploits and Advanced Persistent Threats (APTs).

Building on these concepts, Rid and McBurney suggest a working definition: *"A cyber weapon is any apparatus, device, or set of instructions employed during a conflict to cause direct or indirect harm to physical or digital systems or to degrade the critical infrastructures of a targeted entity."*[70] Cyber weapons are not monolithic but can be categorised into two distinct types based on their design and intent.[71] On the one hand, we have dedicated cyber weapons. These weapons are specifically designed to target a precise objective. They can be likened to firearms; they are purpose-built and tailored for a specific offensive task. A prominent example previously analysed is the Stuxnet worm. Stuxnet represents a paradigm shift in deploying cyber weapons, as it achieved physical destruction without traditional military intervention.

On the other hand, we have repurposed cyber weapons: these are hardware or software tools that were initially passive or defensive, intended to secure information systems, but can be adapted for offensive purposes when necessary. Using an analogy, a repurposed cyber weapon can be compared to the defensive walls of a medieval plains city. As long as control of the walls is maintained, they provide a defensive advantage. However, once the enemy breaches and takes control of the walls, the defenders inside the city are placed at a significant disadvantage. For example, software initially developed for network monitoring can be modified as a tool for espionage or disruption, highlighting the dual-use nature of many modern technologies.

The advent of cyber weapons has significantly altered the dynamics of warfare. This shift reflects what scholars term the *"depoliticisation of violence"*[72], where power is wielded through non-physical means. The rise of Information and Communication Technologies (ICTs)[73] has

---

[70] Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, *157*(1), 6–13. https://doi.org/10.1080/03071847.2012.664354

[71] S. MELE, "Cyber-Weapons: aspetti giuridici e strategici", op. cit., p. 10-11

[72] Cristiano F. (2023). The Blurring Politics of Cyber Conflict: A Critical Study of the Digital in Palestine and Beyond. Lund University.

[73] ICTs is a broader term for Information Technology, which refers to all communication technologies, including the internet, wireless networks, cell phones, computers [...] and other media applications and services enabling users to access, retrieve, store, transmit, and manipulate information in a digital form. Source: Food and Agriculture Organization for the United Nations

further exacerbated this trend, providing state and non-state actors with unprecedented capabilities to engage in cyber operations. Rid and McBurney observe that *"the proliferation of ICTs has not only democratised access to advanced tools but also increased the vulnerability of highly interconnected and resource-rich societies"* [74]. This dual effect has profound implications for global security. As critical infrastructures, such as energy grids, financial systems, and transportation networks, become increasingly reliant on digital systems, they also become prime targets for cyberattacks.

The deployment of cyber weapons raises profound legal and ethical questions. Unlike traditional weapons, cyber weapons often operate within a grey zone, where attribution and accountability are challenging. According to Rid and McBurney, *"the difficulty of attribution in cyberspace complicates the application of international law, creating ambiguities in assigning responsibility for cyberattacks"* [75]. Furthermore, civilian tools can easily be repurposed for malicious activities, blurring the line between peaceful and hostile applications.

Cyber weapons are reshaping the landscape of modern warfare, offering states and other actors new means to exert power and influence. Their unique characteristics, coupled with the complexities of attribution and regulation, pose significant challenges to global security. As Rid and McBurney aptly state, *"Cyber weapons embody the intersection of technological innovation and strategic intent, redefining the parameters of conflict in the 21st century"* [76].

1.6. Different types of cyber activities: cyber exploitation, cyber espionage, and cyber attack

In cybersecurity, it is crucial to understand the distinctions between "*Cyber espionage," "Cyber exploitation"*, and *"Cyber attacks"* is crucial. While interconnected, these activities differ in their intent, execution, and implications under international law and operational practices.

Cyber attacks and exploitations are two primary hostile actions against computer systems or networks. Although they are often grouped under the umbrella term cyber attacks, they are fundamentally distinct. According to the National Research Council (NRC) Report[77], a *cyber attack* involves deliberate actions intended to *"alter, disrupt, deceive, degrade, or destroy*

[74] Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, *157*(1), 6–13. https://doi.org/10.1080/03071847.2012.664354
[75] *Ibidem.*
[76] *Ibidem.*
[77] Owens W.A. et al. (2009). NAT'L Research Council, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 1. NRC Report

computer systems or networks or the information and/or programs resident in or transiting these systems or networks" [78]. A cyber attack's primary goal is to diminish adversary systems' utility or reliability, rendering them unavailable or untrustworthy.

In contrast, cyber exploitation is defined as *"the use of cyber offensive actions… usually to obtain information resident on or transit through an adversary's computer systems or networks"*[79]. Unlike cyber attacks, which are inherently destructive, cyber exploitation focuses on intelligence gathering. To maintain operational secrecy, cyber exploitation is typically designed to avoid disrupting the normal functioning of the targeted systems. Despite these distinctions, cyber attacks and cyber exploitations share operational similarities. Both require access to system vulnerabilities, and the intelligence-gathering process necessary to exploit these vulnerabilities is often identical, as stated in the NRC Report of 2012. However, the payload execution differs significantly. Cyber exploitation prioritises clandestine operations to avoid detection, whereas secrecy is often less critical for cyber attacks, as their effects are typically evident to the target. This overlap in methodologies makes it challenging to distinguish between an act of exploitation and an attack, particularly when the perpetrator's intent remains unclear.

Adding to this complexity is the role of cyber espionage, which is often viewed as a subset of cyber exploitation. Espionage is not classified as an illegal activity under international law. As noted by Hays Parks, espionage is widely practised by all nations and is regulated primarily through domestic laws that prohibit intelligence gathering within a nation's borders without categorising it as a violation of international norms[80]. Cyber espionage is typically conducted digitally, leveraging vulnerabilities to access sensitive information. Nations generally recognise cyber exploitation as a new method of espionage, permissible under the Law of Armed Conflict (LOAC)[81], even if such activities inadvertently support subsequent cyber-attacks.

The interaction between these cyber activities creates significant challenges for attribution and response. Vulnerabilities exploited for espionage or intelligence purposes can later be weaponized for destructive cyber attacks, often leaving the targeted party uncertain about the

---

[78] Wortham, Anna (2012) "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?," Federal Communications Law Journal: Vol. 64: Iss. 3, Article 8. Available at: https://www.repository.law.indiana.edu/fclj/vol64/iss3/8

[79] *Ibidem.*

[80] *Ibidem.*

[81] The Law of Armed Conflict is the law that regulates the conduct of participants during an armed conflict. This law includes rules for the protection of victims of armed conflict, i.e those who do not or who no longer participate in hostilities, and also rules regulating the means and methods of warfare. Source: Oxford Institute of ethics, Law and Armed Conflict.

nature of the initial breach. As the NRC Report 2012 highlights, *"Even when an action is limited exclusively to cyber exploitation, the potential to use that same vulnerability for a later cyber attack is still present"*[82]. This dual-use nature of cyber tools complicates determining whether an act constitutes exploitation, attack, or both.

This ambiguity raises critical legal and policy questions. For example, does introducing vulnerabilities into an adversary's systems constitute a threat of force under the UN Charter? Does the mere discovery of a vulnerability justify anticipatory self-defence?

Furthermore, equipping a cyber exploitation tool with attack capabilities is minimally expensive, and adversaries often integrate these capabilities regardless of whether they will be used. This overlap in functions further complicates a targeted party's ability to determine the nature of the threat they face.

1.7. Defining the Importance of Critical Infrastructures

As mentioned, in recent years, cyberspace has experienced rapid and unprecedented growth, evolving into a vast, dynamic, and intricate network of interconnected devices. This transformation has profoundly impacted critical infrastructure systems, which serve as the backbone of modern society. Historically, critical infrastructures were considered resilient to cyber threats due to their reliance on proprietary networks and specialised hardware. However, this perception has been upended by a surge in sophisticated cyberattacks, exposing vulnerabilities that have only been amplified by the shift to open standards and web-based technologies.

The growing frequency and sophistication of cyberattacks on critical infrastructure underline the urgency of addressing these vulnerabilities. High-profile incidents targeting oil pipelines, hospitals, and government websites reveal the devastating potential of such breaches. These attacks disrupt essential services and result in loss of life, economic instability, and threats to national security[83].

---

[82] Wortham, Anna (2012) "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?," Federal Communications Law Journal: Vol. 64: Iss. 3, Article 8. Available at: https://www.repository.law.indiana.edu/fclj/vol64/iss3/8

[83] Johnson.T.A. (2015). Cybersecurity. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Webster University, St. Louis, Missouri, USA.

To effectively address the growing threats to critical infrastructures, it is first essential to establish a clear and consistent definition. However, it is essential to recognise that the definition of critical infrastructure and its associated sectors varies between countries, reflecting differences in priorities, national contexts, and evolving threat landscapes. All the definitions share standard features and the idea that infrastructures serve as foundational systems enabling various human activities, mainly economic functions, as well as those essential for security and public health. Critical infrastructures can be likened to *"the skull and bones of a body, to its blood vessels, to its nervous system: in short, to its vital organs, which need to be in place and work well for every action of the human body to be performed efficiently and painlessly."* [84]

Within the European Union, the definition of critical infrastructure has evolved significantly, mirroring the EU's adaptive approach to addressing modern risks and enhancing resilience.

The now-abrogated Council Directive 2008/114/EC of 8 December 2008, in Article 2, defined critical infrastructure as:

> *"European critical infrastructure (ECI) means an asset, system or part thereof located on EU territory, which is essential for the maintenance of vital societal functions, health, safety, security, economic or well-being of people, and the disruption or destruction of which would have a significant impact on at least two Member States, as result of the failure to maintain those functions.*
>
> *The significance of the impact is assessed against distinct cross-cutting criteria, which encompass casualties, economic and environmental effects, and public effects."*[85]

While this definition provided an essential foundation for addressing the protection of critical infrastructure in the EU, the Council Directive 2008/114/EC was repealed with the adoption of the Directive (EU) 2022/255 of the European Parliament and of the Council of 14 December 2022[86]. The new directive introduced a broader and more refined framework for resilience, shifting focus from the protection of physical assets to the resilience of critical entities that

[84] Viganò, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of Critical Infrastructure. In International Library of Ethics, Law and Technology (pp. 157-177). (International Library of Ethics, Law and Technology; Vol. 21). Springer. https://doi.org/10.1007/978-3-030-29053-5_8

[85] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[86] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

provide essential services. The Directive (EU) 2022/2557 introduces several vital terms reflecting this expanded resilience approach. According to Article 2, paragraphs (1), (4) and (5), the following definitions are central to the framework:

> *(1) 'critical entity' means a public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex;*
> *(4) 'critical infrastructure' means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service;*
> *(5) 'essential service' means a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment;*[87]

This transition from the 2008 to the 2022 directive represents an evolution in the EU's approach to securing critical infrastructure. The new focus on critical entities and essential services highlights the importance of identifying and protecting the systems and actors that underpin societal resilience rather than limiting the scope to physical infrastructure alone.
The United States has, from the outset, adopted a broad and inclusive approach to critical infrastructures (CIs), mainly influenced by the events of September 11, 2001. The U.S. Patriot Act defines CIs as:

> *"systems and assets, whether physical or virtual, so vital to the U.S. that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."* [88]

This highlights the emphasis on the essential role CIs play in ensuring national security and societal stability. The Homeland Security Act of 2002 refined this framework by establishing the Department of Homeland Security (DHS)[89] and introducing the concept of *"key resources"*.

[87] European Parliament and Council (2022). *Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.* Official Journal of the European Union, L 333, 27 December 2022, pp. 164–195. Article 2 Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2557/oj.
[88] National Institute of Standards and Technology (NIST). Critical Infrastructure.
[89] The Department of Homeland Security (DHS) works to improve the security of the United States. The Department's work includes customs, border, and immigration enforcement, emergency response to natural and manmade disasters, antiterrorism work, and cybersecurity. Source: USA.gov

These resources, which may be publicly or privately controlled, are described as essential to the minimal functioning of the economy and government. While the act does not explicitly enumerate what constitutes key resources, it treats them as distinct from CIs yet equally deserving protection. This dual emphasis on CIs and key resources underscores the United States' comprehensive approach to safeguarding its foundational systems and assets.

In other words, the term critical infrastructure refers to a network of essential systems and structures that underpin the operation of industrialised nations, ensuring a continuous flow of goods and services vital for organisational efficiency, operational functionality, and economic stability. Essential services are intended for the collective benefit and encompass public and private entities. They form a cornerstone of a nation's social and economic well-being, making them indispensable and safeguarded by the state[90]. The significance of critical infrastructure lies in the fact that its destruction or even temporary disruption could have devastating consequences, not only for the economy and a nation's defence capabilities but also for the daily lives of its citizens. It becomes clear that the security, development, and quality of life in industrialised nations are closely tied to these systems' continuous and coordinated operation, deemed "critical" due to their strategic importance[91].

In the books *Critical Infrastructure Protection in Homeland Security: Defending a Networked Infrastructure* by Ted G. Lewis[92] and *Critical Information Infrastructures Resilience and Protection* by Maitland Hyslop[93] is evident how modern Western countries have developed over the years a societal model characterised by a high "quality of life". This expression refers to the ability to access various services provided to every individual, allowing them to meet their primary and secondary needs. These services include, for example, energy supply, healthcare, transportation systems, banking, drinking water, and more. In recent years, those infrastructures (now considered commodities) that enable the delivery of services that define the quality of life, both for citizens and businesses, whether public or private, have become increasingly indispensable.

The infrastructure system encompasses a wide range of categories and sectors. Within critical infrastructure, the following sectors can be identified: energy production, transportation, and distribution systems; telecommunications infrastructure; transportation networks; healthcare

[90] Brocardi, Dizionario giuridico, “Servizi pubblici essenziali”
[91] *Ibidem.*
[92] Lewis T.G. (2014). Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. Second Edition.
[93] Hyslop M. (2007). Critical Information Infrastructures. Resilience and Protection. Springer.

systems; banking and financial circuits; water collection, distribution, and treatment infrastructure; the food supply chain; and emergency services.

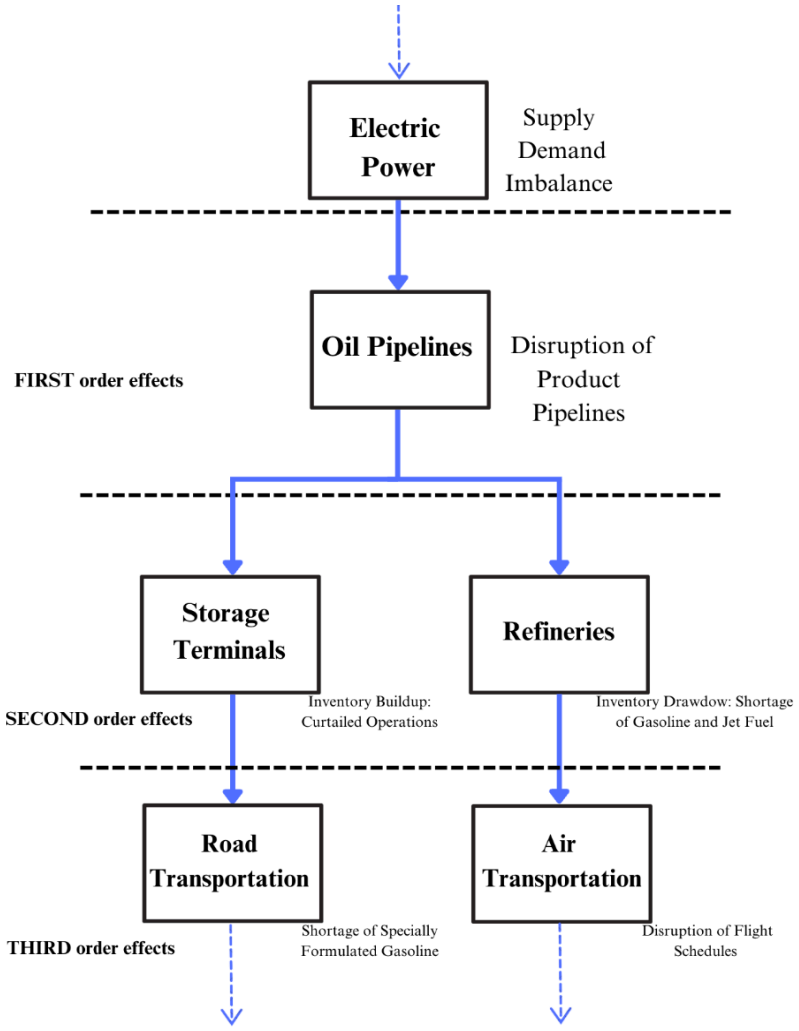
Each sector is supported by its infrastructure, such as highway transportation networks or energy systems for generating and distributing electricity. Critical infrastructure in these areas represents a significant commitment of public resources. Determining and categorising a country's critical infrastructure involves identifying and prioritising key sectors and assets based on their essential role in maintaining national stability and security.

Critical infrastructure (CI) sectors are integral components of a complex and interdependent system, which, while essential to modern society, is also increasingly vulnerable to threats. Historically, these sectors operated independently, functioning as autonomous entities. However, the evolving economic, social, and technological landscape has fostered greater interconnectivity, resulting in what is often described as the "domino effect".[94] This phenomenon highlights how the disruption or failure of one critical infrastructure can cascade across the entire system creating severe consequences for both society and the economy.

Interdependencies among CI sectors are multifaceted. For example, two infrastructures might be physically, geographically, or logically interconnected. Additionally, they can display cyber interdependence, where the performance of one sector depends on information transmitted through cyberspace. Such interconnections mean that an attack on one sector, such as energy, would inevitably affect others, amplifying the overall impact, as displayed in Figure 2. This dynamic necessitates that interdependencies be carefully accounted for in protective programs, as the disruption of one sector can propagate and endanger the stability of multiple others.

[94] Kadri F. - Birregah B. & Châtelet E. (2014). "The Impact of Natural Disasters on Critical Infrastructures: A Domino Effect-based Study," Journal of Homeland Security and Emergency Management, De Gruyter, vol. 11(2), pages 217-241.

Figure 2: Cascading consequence example (adapted from Rinaldi et al., 2001)[95]



To address these challenges, enhancing critical infrastructure protection requires systematic monitoring of incidents across all sectors, maintaining robust databases of vulnerabilities, and integrating these databases with threat analysis. Countries with extensive infrastructure systems, like the United States, have implemented such measures. Federal agencies collaborate with each CI sector to support the development and execution of protective strategies. A key component of this process involves recording and analysing attacks on critical infrastructure, along with their consequences, to strengthen preparedness and mitigate future risk[96].

[95] Kovacevic A. - Nikolic D. (2015). Cyber Attacks on Critical Infrastructure: Review and Challenges. University of Belgrade.
[96] *Ibidem.*

1.8. Vulnerabilities and Risks of Critical Infrastructures

Critical infrastructures are inherently vulnerable to various risks that can be exploited for cyberattacks. Key vulnerabilities include[97]: *(i)* complexity of systems: many critical infrastructures rely on highly complex and customised industrial control systems (ICS), which are challenging to secure and update; *(ii)* outdated security systems: many ICS and software systems depend on outdated IT technologies not designed with modern cybersecurity protocols in mind; *(iii)* lack of segmentation: poor segmentation and inadequate management of IT and operational technology (OT) networks make it easier for ransomware and malware to penetrate and spread; *(iv)* dependency on suppliers: large organisations managing critical services, such as energy or water supply, often face security gaps due to reliance on external suppliers and *(v)* limited visibility: insufficient visibility into resources, network traffic, and threats across IT and OT environments, especially when using heterogeneous and non-standard systems, further exacerbates risks.

These vulnerabilities and the growing sophistication of cyber threats expose critical infrastructure to significant risks.: Namely, operational disruptions refer to system shutdowns or the inability to deliver essential services; sensitive data compromise results in the theft of intellectual property or personal data; physical damage is the potential harm to infrastructure or threats to public safety, while financial losses are the costs related to recovery, litigation, and reputational damage. As a result, business leaders and government policymakers must prioritise investments in cybersecurity (training, fostering a specific security culture, and engaging experts and specialised companies) to improve the operational resilience of systems and mitigate risks threatening critical infrastructures. The interconnected nature of critical infrastructures and greater reliance on ICT systems[98] for management, maintenance, and remote control significantly heightens exposure to cyber threats. Industrial control systems, which manage critical infrastructures like power plants, dams, gas facilities, and railways, are often connected to standard IT networks. While this integration reduces costs and improves flexibility, it also increases the risk of cyberattacks, potential traffic issues, and service degradation. Consequently,

[97] The President's National Infrastructure Advisory Council (2017). Securing Cyber Assets. Addressing Urgent Cyber Threats to Critical Infrastructure. NIAC

[98] CT, or information and communications technology (or technologies), is the infrastructure and components that enable modern computing. Among the goals of IC technologies, tools and systems is to improve the way humans create, process and share data or information with each other. Source: TechTarget

securing critical infrastructures has become a national priority and a complex challenge requiring collaboration between governments and the private sector.

As noted, critical infrastructures are often managed by control systems. Early control networks were relatively simple, featuring direct point-to-point connections between monitoring or command devices and remote sensors or actuators. Over time, these systems evolved into sophisticated networks that enable centralised communication between a control unit and numerous remote units operating on a shared communication bus[99].

One system requiring particular attention is Supervisory Control and Data Acquisition (SCADA), widely used to manage critical infrastructures in transportation systems, water and wastewater treatment, electric distribution, oil and natural gas distribution, and many more. Therefore, if SCADA malfunctions, it will have a debilitating impact on the community and society. SCADA systems perform two tasks: centralised monitoring of the system and control of it[100]. These systems gather, store, and analyse data based on predefined parameters established by human operators. If any abnormal activity is detected, it either issues commands or alerts the operator. These systems can include thousands of components designed to monitor and control processes, including sensors, actuators, and Programmable Logic Controllers (PLC)[101]. Modern SCADA systems have increasingly become high-profile targets for cyberattacks. Their integration with organisational IT infrastructures and the Internet has enhanced operational efficiency and cost savings but also introduced significant security vulnerabilities. The emergence of advanced malware, such as Stuxnet, underscores the limitations of relying solely on traditional IT-based security mechanisms.

While SCADA systems share similarities with IT systems, they have unique operational demands that make conventional security solutions less effective. For example, SCADA systems often require uninterrupted availability, face strict real-time performance requirements, and can be difficult to update, leaving them vulnerable to threats.

Historically, SCADA systems prioritised physical security over network security and were often isolated from external networks. However, *"today, there is a high demand for interconnectivity*

[99] Kovacevic A. - Nikolic D. (2015). Cyber Attacks on Critical Infrastructure: Review and Challenges. University of Belgrade.
[100] *Ibidem.*
[101] A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. Source: National Institute of Standards and Technology.

between SCADA systems and corporate networks" [102], significantly increasing their exposure to cyber threats. The shift from proprietary to open standards in SCADA communication has further exacerbated this issue. Open standards make it easier for attackers to gain detailed knowledge about SCADA networks, increasing their susceptibility to infiltration.

One significant challenge is the widespread adoption of commercial off-the-shelf (COTS) hardware and software in SCADA systems. While COTS technology reduces costs and accelerates development, it raises concerns about the overall security of the final product. Attackers often exploit vulnerabilities in shared protocols, such as Ethernet and TCP/IP[103], to infiltrate systems.

The interconnected nature of SCADA systems with corporate IT infrastructures has also increased the access points for attackers. These vulnerabilities enable attackers to block or delay the flow of information through control networks or make unauthorised changes to programmed instructions in the PLCs, RTUs, and DCS controllers[104]. Such disruptions can result in the malfunctioning of essential infrastructure, including energy and water distribution systems. Beyond operational risks, cyberattacks on critical infrastructure can have wide-ranging consequences, including direct financial consequences of a cyber incident and reputation and impact on health, safety, the environment, and even human life.

The geographical concentration of critical assets poses significant risks, among other vulnerabilities. Many critical infrastructures are clustered within specific regions, amplifying their susceptibility to localised disruptions or cascading failures. Politically motivated or state-sponsored attacks further exacerbate these risks, targeting critical services and posing significant national security and stability challenges.

1.9. Cyber Attacks on Critical Infrastructures

Threats to critical infrastructures can be categorized into three distinct groups: natural, human-caused, and accidental or technical threats. In this context, we will focus exclusively on the second category: human-caused threats, specifically those carried out through cyberattacks.

[102] Kovacevic A. - Nikolic D. (2015). Cyber Attacks on Critical Infrastructure: Review and Challenges. University of Belgrade.p.5

[103] Transmission Control Protocol/Internet Protocol. TCP/IP is a set of standardized rules that allow computers to communicate on a network such as the internet. Source: AVAST.

[104] Robles R. J. et al. Common Threats and Vulnerabilities of Critical Infrastructures. International Journal of Control and Automation.

Cyber-attacks are a progression of physical attacks: they are cheaper, less risky for the attacker, not constrained by distance, and easier for replication and coordination[105]. The most common cyber threats include phishing campaigns, spreading destructive malware (especially ransomware), DDoS attacks, misinformation campaigns, and data leaks from central databases. Exploiting vulnerabilities, including those that are known but not adequately addressed, is one of the most frequent intrusion methods, facilitating the unauthorised entry of hostile actors into the security perimeter of critical infrastructures and significant institutional websites.

Cyber threats to critical infrastructures continue to grow in terms of frequency, scope, and technical sophistication more in detail they use various attack vectors, including malware (i.e. viruses, ransomware, spyware, and other malicious code designed to disrupt or slow operations or damage systems), Denial-of-Service (DoS) attacks (i.e. attacks are designed to overwhelm websites and networks with false traffic and requests to prevent access by legitimate users and limit service delivery); supply chain attacks (i.e. targeting weaker external suppliers and partners in an organisation's supply chain to penetrate internal networks); social engineering (i.e. manipulating users within an organisation to reveal sensitive information or download malicious malware) and web application attacks (i.e. exploiting known vulnerabilities in operating systems and web applications exposed on the internet to access data and silently exfiltrate sensitive information). Furthermore, cyber attacks on SCADA systems can be classified as[106]: *(i)* Non-targeted attacks (i.e. incidents that occur due to common threats affecting any device connected to the internet. These types of attacks are not aimed at a specific target. However, they can still cause significant damage, such as the Slammer worm infecting the Davis-Besse nuclear power plant) and *(ii)* targeted attacks (i.e. carefully crafted attacks to disrupt or damage the physical systems controlled by the targeted SCADA system. These attacks, such as the one promoted by Stuxnet malware, are particularly hazardous for critical infrastructure because they are strategically designed to target and disrupt particular organisations, often within industries where the consequences of such disruptions can be especially devastating).

Attacks on SCADA systems are continually increasing. The British Columbia Institute of Technology in Canada created a database of SCADA security incidents: the BCIT Industrial Security Incident Database (ISID). What is evident is that before 2000, most incidents (70%) were either due to accidents or disgruntled insiders acting maliciously. Between 2001 and 2004,

[105] Kovacevic A. - Nikolic D. (2015). Cyber Attacks on Critical Infrastructure: Review and Challenges. University of Belgrade.
[106] *Ibidem.*

almost 70% of the incidents were attacks from outside SCADA systems[107]. According to Kaspersky's ICS-CERT 2023 Report, nearly 40% of Industrial Control Systems (ICS), including SCADA systems, experienced malicious activity globally[108]. The Dragos 2023 Year in Review highlights that the energy sector, heavily reliant on SCADA, remains the most targeted, with ransomware attacks directly aimed at disrupting operations and pressuring victims to pay[109]. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) reported a significant uptick in vulnerabilities affecting SCADA systems, driven by the rapid adoption of internet-connected devices, expanding the attack surface for potential threats[110]. These trends underscore that SCADA threats remain a pressing concern for critical infrastructure security.

Cyber attacks on critical infrastructures are divided into various categories based on the method of operation, impact, and the perpetrators behind these attacks. The following table[111] includes the categorisation of the relevant information.

Table 1: Categorization of Cyber Attacks on Critical Infrastructures:
Methods, Impacts, Perpetrators, and Targeted Sectors.

Method of operation (MO)	Impact	Perpetrators	Critical Infrastructure Sector
Misuse of Resources User Compromise Root Compromise Web Compromise Social Engineering Malicious code (Virus, Trojan, Worm, Spyware, Arbitrary code execution) Denial of Service Others	Disrupt Distort Destruct Disclosure Death Unknown	Hackers Terrorists Disgruntled employees/inside attacks Hobbyists/Script kiddies Hacktivists Unknown	Agriculture and food Water Public health and safety Emergency services, Government Defense industrial base Information and telecommunications Energy Transportation Banking and finance Industry/manufacturing Postal and shipping.

The method of operation has a different level of impact and requires specific defensive strategies. The Impact category describes the outcomes of these attacks. These can range from minor disruptions to major system failures that lead to economic or safety consequences. The impact of an attack is crucial in understanding the severity of the threat posed to CI and its

[107] *Ibidem*.
[108] Kaspersky Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Threat Landscape for Industrial Automation Systems: Statistics for H2 2023.
[109] Dragos, Inc. (2023). ICS/OT Cybersecurity Year in Review.
[110] Cybersecurity and Infrastructure Security Agency (CISA). Known Exploited Vulnerabilities Catalog.
[111] Kovacevic A. - Nikolic D. (2015). Cyber Attacks on Critical Infrastructure: Review and Challenges. University of Belgrade.

surrounding systems. Perpetrators are another key element which has been discussed previously in this chapter. The above table categorises various types of attackers, such as hackers, terrorists, and disgruntled employees. It helps refine the understanding of how threats emerge and offers insights into the potential for future attacks. As we analyse these categories, we focus on understanding the specific Critical Infrastructure Sectors targeted by these attacks. By doing so, we can identify the most vulnerable sectors and implement the necessary protections. For example, the energy, telecommunications, and transportation sectors are at high risk due to their centrality in modern life and the consequences of their disruption.

This chapter has explored the role of cyberspace as a key domain of modern security, the increasing threats to critical infrastructures and the actors behind cyber warfare, espionage, and attacks. The growing interconnectedness of essential sectors has amplified vulnerabilities, making cybersecurity a strategic priority. As digital dependence deepens, the challenge is no longer just about preventing attacks but about fostering resilience, ensuring that societies can adapt and respond effectively to an ever-changing threat landscape. The rapid evolution of cyber threats also raises ethical and legal dilemmas, particularly regarding state accountability, civilian protection, and the blurred lines between cyber defence and cyber offence. Addressing these challenges requires more than just technological solutions, it necessitates a coordinated global effort that balances security, privacy, and international stability. To address these challenges, Chapter 2 will examine the regulatory frameworks at national and international levels. Focusing on NATO's Article 5, the evolution of European cybersecurity laws from the NIS Directive to NIS2, and the cooperation between the EU and NATO in strengthening cyber defence. These measures reflect an ongoing effort to redefine security in an age where digital vulnerabilities can have tangible geopolitical consequences.

CHAPTER II

Cybersecurity: The Regulatory Framework in Europe and NATO

2. Introduction

Building upon the understanding of cyberspace and its security challenges explored previously, this chapter focuses on the regulatory frameworks developed to address these threats at the European and NATO levels. Legal and institutional mechanisms have become essential elements of national and international security strategies. The discussion begins by examining cybersecurity as an essential component of national security and the necessity of comprehensive regulatory measures to mitigate digital vulnerabilities.

The chapter then delves into the European Union's cybersecurity framework, tracing its evolution from early legislative efforts to the adoption of the *NIS* and *NIS2 Directives*. It also examines the *Cyber Resilience Act* and other key initiatives to strengthen the resilience of critical infrastructures. The chapter explores how the EU's approach has transitioned from fragmented national policies to a harmonised, risk-based strategy emphasising cooperation, resilience, and proactive defence mechanisms.

Following this, the chapter analyses NATO's role in cybersecurity governance. As a military alliance primarily focused on collective defence, NATO has had to adapt its strategic posture to the realities of cyber warfare. The chapter examines how NATO has integrated cyber threats into its defence doctrine. It explores key developments such as establishing the *Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, the recognition of cyberspace as an operational domain, and the potential invocation of Article 5 in response to significant cyber incidents.

The chapter then explores the strategic partnership between the EU and NATO in addressing cyber threats. Given cyberspace's transnational nature, effective cybersecurity requires coordinated international responses. The discussion highlights joint initiatives, policy alignments, and institutional collaborations to strengthen cyber resilience and critical infrastructure protection across the Euro-Atlantic region. The chapter concludes by formulating the research puzzle, main research question, and hypothesis that guide the case study of Ukraine in Chapter III.

2.1. Cybersecurity as a Pillar of National Security: The Need for Regulatory Frameworks

National security has traditionally been understood as a state's ability to defend itself against external threats, predominantly of a military nature. However, with the evolution of modern society and the advent of the digital era, this perspective has proven inadequate. Today, threats to a state's stability no longer stem solely from armed attacks but manifest in more sophisticated and pervasive forms, exploiting the dependence of critical infrastructures on interconnected systems. As a result, the very concept of security has expanded, encompassing four interrelated dimensions: external security, internal security, environmental security, and virtual security.[112] The increasing complexity of modern threats has led scholars and policymakers to emphasise the interconnectedness between security and other facets of national well-being. As Petrișor Pătrașcu (2022) aptly notes in *Romanian Military Thinking*, a journal published by the Romanian Defence Staff:

> *"Security is one of the most important objectives of national interest, which contributes to the achievement of other objectives, such as prosperity (social well-being), national values, or international stability. At the same time, there is a relationship of interdependence between security and prosperity, in the sense that through the economic-financial means the capabilities for defence, public order, national security and intelligence can be ensured."*[113]

The evolving nature of national security, where economic resilience, technological capabilities, and institutional frameworks are equally critical alongside traditional defence mechanisms, is clearly expressed. Such an understanding is particularly relevant in cybersecurity, where safeguarding critical infrastructures is not merely a technological challenge but a fundamental pillar of national stability.

For what concerns the four interrelated dimensions, external security focuses on a state's ability to safeguard its territorial integrity against military threats[114]. It has traditionally been considered

[112] Drent M., et al. (2014). The Relationship between External and Internal Security. Clingendael, Netherlands Institute of International Relations.

[113] Pătrașcu, P. (2022) National security strategies and critical infrastructure: An analysis of the European Union member states, *Romanian Military Thinking*, 3, p. 12.

[114] Herz, J. (2003)'The security dilemma in international relations: background and present problems', International Relations 17(4), pp.411−16.

the cornerstone of national security. It plays a central role in realist international relations theory, which asserts that a state's survival depends on its capacity to protect itself from hostile actors and maintain a balance of power[115]. This paradigm has long dominated national defence strategies, prioritising military strength as the primary security instrument. However, in the contemporary era, external security can no longer be assessed solely regarding military deterrence and conventional defence. The evolution of threats has required a more complex approach[116]. A state's protection now depends on its ability to withstand direct attacks and its resilience against emerging forms of aggression. These include cyberattacks and hybrid operations that combine cyber warfare, disinformation, and economic sabotage[117].

Equally fundamental is internal security, which pertains to a state's political, institutional, and social stability[118]. A stable political system, legitimate institutions, and the state's ability to prevent internal conflicts are essential for ensuring national cohesion. Unlike external security, which focuses on threats posed by foreign actors, internal security addresses tensions that may arise within national borders, such as insurgencies, domestic terrorism, organised crime, and cyberattacks aimed at destabilising institutions[119]. The increasing use of technology for subversive activities, ranging from disinformation campaigns to cyberattacks on electoral systems, has made this dimension particularly vulnerable. Failure to maintain internal stability and respond effectively to such challenges exacerbates a state's fragility, making it more susceptible to external threats.[120]

Another growing important dimension is environmental security, which pertains to a state's ability to safeguard its natural resources and ensure environmental sustainability in the face of climate change, water and energy resource management, and ecosystem preservation. Environmental security is closely linked to economic and social stability: extreme weather events, water crises, or conflicts over resource access can trigger political instability, forced migration, and geopolitical tension. The interdependence between environmental security and cybersecurity is becoming increasingly evident: critical infrastructures such as power grids, water treatment plants, and transportation systems are becoming even more digitised and, consequently, more vulnerable to cyberattacks. For instance, a cyberattack targeting an energy

[115] Waltz, K.N. (1979) *Theory of International Politics*. Reading, MA: Addison-Wesley.
[116] Reese B. (2024) Balanced Realism: A 21st Century Approach to International Relations Theory. Medium.
[117] Kegley, C.W., Jr. and Raymond, G.A. (2021) Realism in the age of cyber warfare, *Ethics & International Affairs*.
[118] Jackson-Preece J. (2011) Security in International Relations. University of London.
[119] Kolodziej Edward A. (2005) Security and International Relations. Cambridge University Press.
[120] Digmelashvili T. (2023) The Impact of Cyberwarfare on the National Security. Future Human Image, Volume 19, 12-19.

distribution network or a power plant could have devastating consequences for environmental security and public well-being[121].

Finally, virtual security (i.e., cybersecurity) is the most recent of the four dimensions, yet it has rapidly become one of the most critical. Defined as a state's ability to protect itself and its institutions from cyber threats, espionage, sabotage, digital crime, and attacks on strategic infrastructure, cybersecurity is now a cornerstone of national security. Information networks and digital systems are at the heart of every key sector, from finance to defence, from healthcare to industry.[122] The vulnerability of these systems extends beyond the technological sphere, directly impacting a country's political and economic stability. For this reason, ensuring cyberspace security has become a priority for governments and institutions, which must address increasingly complex challenges related to data protection, the resilience of critical infrastructures, and defence against highly sophisticated cyberattacks[123].

The traditional deterrence framework, rooted in the logic of nuclear strategy and conventional military power, faces unique challenges in the cyber domain. Unlike kinetic weapons, cyber capabilities are relatively low-cost, easily deployable, and often covered in ambiguity due to attribution difficulties. This has introduced the concept of *deterrence by denial*, whereby states invest heavily in defensive measures to prevent successful intrusions rather than relying solely on the threat of retaliation[124]. Moreover, emerging technologies, such as artificial intelligence (AI) and quantum computing, are reshaping the strategic landscape. AI can enhance threat detection and response through sophisticated pattern recognition, yet it also raises the stakes by potentially enabling the automation of cyberattacks. Similarly, quantum computing threatens to upend current cryptographic systems, compelling governments and industries to explore post-quantum encryption methods[125]. These developments necessitate reexamining deterrence theory in the digital age and underscore the need for adaptive security policies that balance offence, defence, and resilience. States must go beyond protecting physical infrastructures, adopting a systemic approach to ensure cybersecurity in all sectors.

---

[121] Cybersecurity Guide Contributors (2024). Safeguarding the environment: Cybersecurity in environmental protection. Cybersecurity Guide.

[122] Digmelashvili T. (2023) The Impact of Cyberwarfare on the National Security. Future Human Image, Volume 19, 12-19.

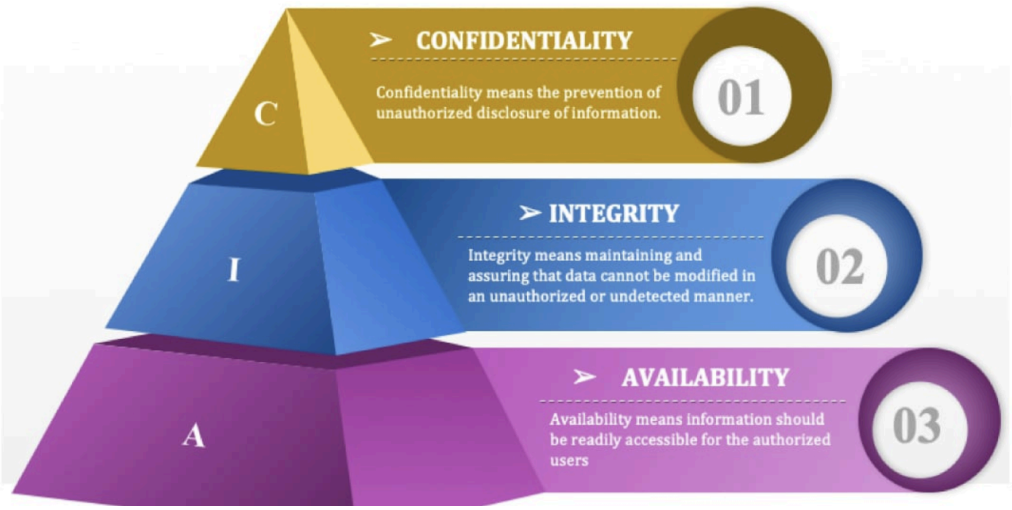
[123] *Ibidem.*

[124] Borghard, E. D. and Lonergan, S. W. (2021) Deterrence by denial in cyberspace, *Journal of Strategic Studies*, 46(3), pp. 534–569. doi: 10.1080/01402390.2021.1944856.

[125] Livelli, F.M.R. (2024)'Cyber security nell'era del quantum computing. Ci si difende così, *Cyber Security 360.*

Several key protection areas can be identified within cybersecurity. Information security ensures that sensitive data remains uncompromised, preserving its confidentiality, integrity, and availability (commonly called the CIA triad).

Figure 3: CIA Triad[126]



Source: Agbeleye O. (2023). What Is Cybersecurity? A Complete Overview Guide. Springboard.

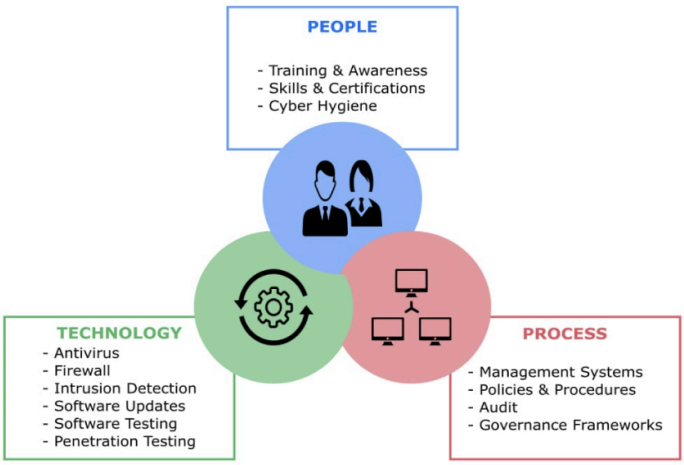
IT security focuses on protecting computer systems and corporate networks, while operational technology (OT) security concerns the defence of industrial control systems and critical networks. On the other hand, Internet of Things (IoT) security seeks to protect connected devices, which constitute an expanding attack surface[127].

An effective cybersecurity strategy is built on three fundamental pillars: people, processes, and technology[128]. Organisations must employ adequately trained cybersecurity professionals to design and implement effective security frameworks. It is essential to provide employees with adequate training to help them recognise phishing scams and social engineering techniques. Human error often represents the weakest link in an organisation's cybersecurity resilience. Processes and policies, in turn, provide the guidelines for cybersecurity governance. These

[126] Agbeleye O. (2023). What Is Cybersecurity? A Complete Overview Guide. Springboard.
[127] Institute for Defence and Business (n.d.) 'Cyber Security and the Internet of Things (IoT)', *Institute for Defence and Business*.
[128] Wilcox S. (2022). Three Pillars of Cyber Security: People – Process – Technology. Open Access Government.

processes include incident response plans, threat analysis, asset prioritisation, and real-time interventions in the event of a cybercrime, enabling the identification and elimination of potential intruders. Finally, technology refers to the IT infrastructure, encompassing both hardware and software, that organisations use to achieve their cybersecurity objectives. Examples include antivirus software and defensive artificial intelligence, which can monitor computer networks for anomalous behaviour and learn from previous attacks to enhance threat detection and response[129].

Figure 4: Three Pillars of Cybersecurity: The Foundation of Effective Cybersecurity[130]



Source: Agbeleye O. (2023). What Is Cybersecurity? A Complete Overview Guide. Springboard.

A further critical consideration is the inherent tension between national sovereignty and the transnational nature of cyberspace. While states have traditionally exercised complete control within their borders, the digital realm defies geographical constraints and often involves actors operating across multiple jurisdictions. This blurring of boundaries challenges conventional notions of state control and encourages policymakers to consider innovative governance mechanisms that transcend national limits[131]. In response, international bodies such as the United Nations, the European Union, and NATO have increasingly sought to develop shared norms and cooperative frameworks. However, the resulting patchwork of regulations, characterised by

[129] *Ibidem.*
[130] Agbeleye O. (2023). What Is Cybersecurity? A Complete Overview Guide. Springboard.
[131] Moynihan H. (2019). The Application of International Law to State Cyberattacks Sovereignty and Non-intervention. Chatham House, The Royal Institute of International Affairs.

varying standards and degrees of binding authority, illustrates the struggle to reconcile sovereign interests with the need for collective action. On this note, it has become a priority for major international organisations. However, cybersecurity governance remains inconsistent on a global scale, characterised by diverse regulations and varying approaches among nations and organisations. While the United Nations has adopted resolutions and initiated working groups to define common principles for cybersecurity, these initiatives often lack binding effectiveness. As a result, the European Union and NATO have taken a leading role in developing a more structured and operational regulatory framework for protecting critical infrastructures. The NIS Directive and its successor, the NIS2 Directive, are the EU's primary legislative instruments for strengthening the resilience of strategic sectors. Meanwhile, NATO has officially recognised cyberspace as an operational domain and has developed defence strategies and response mechanisms to counter cyberattacks that could compromise the security of its member states[132].

2.2. The European Union's Cybersecurity Framework: From NIS to NIS2 and Beyond

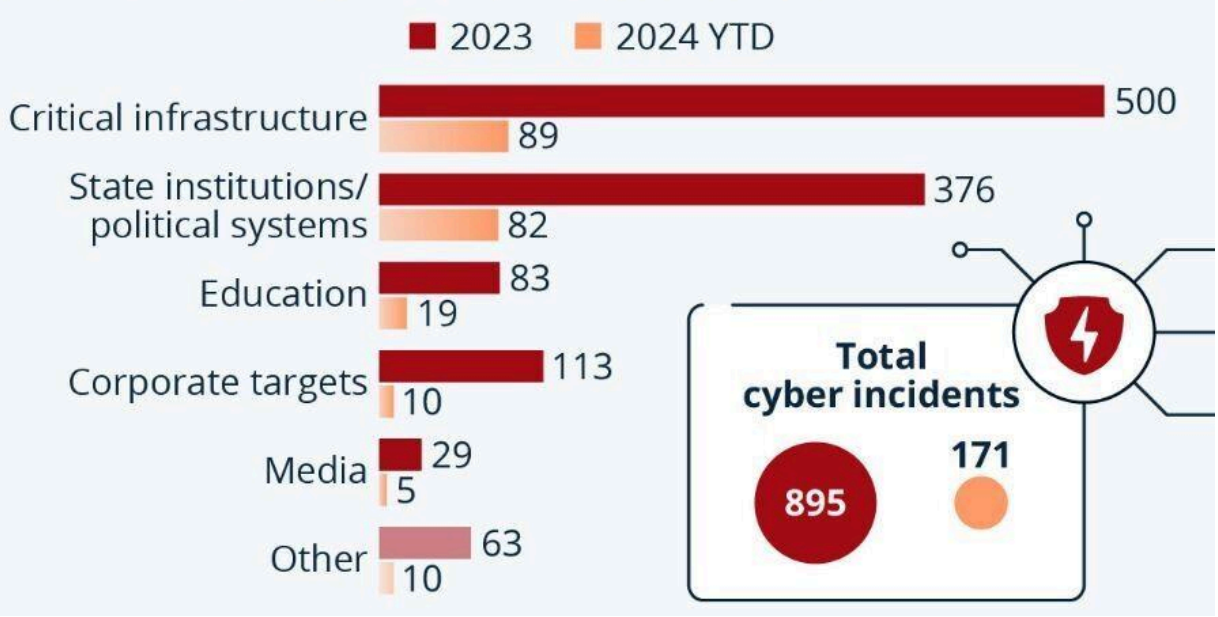
Infrastructure plays a strategic role within the European Union, serving as a key component for the movement of people and goods and as a crucial driver of economic growth and social development. Roads, bridges, railways, and energy networks constitute an essential element of the single market, fostering the EU's global competitiveness. Integrating these systems into the European economic fabric stimulates investment, increases long-term productivity, and necessitates constant attention to their security and resilience. Consequently, the Union has progressively developed policies to ensure the protection and continuous modernisation of critical infrastructure, addressing threats that could undermine its operational stability. In this context, cybersecurity has emerged as an essential facet of infrastructure protection[133].

In a recent study on cybersecurity in Europe (2024) titled *"Shielding the Future: Europe's Cyber Threat Landscape Report"*[134], Cloudflare shares data on how organisations cope with rising volumes of cybersecurity incidents, their levels of preparedness, and top challenges. The survey, which included more than 4,000 business and technology leaders across 13 European markets, found that *"40% of organisations experienced a cybersecurity incident in the last 12 months,"*[135]

[132] Blumfelde S.(2022). The role of international organisations in global cybersecurity governance.
[133] European Commission (2024) Critical infrastructure resilience at EU-level, *Official Website of the European Union.*
[134] Cloudflare (2024). Shielding the Future: Europe's Cyber Threat Landscape Report.
[135] Fitzgerald A. (2024). Understanding EU Cybersecurity: History, Regulations, and Certifications. Secureframe.

with *"84% of that group reporting that the frequency of these events has increased over the same period."*[136] Furthermore, the study highlights that this trend is expected to continue; *"64% of surveyed European business leaders anticipate a cybersecurity incident within the next 12 months, while only 29% believe they are highly prepared to defend against such threats"*[137]. Given this data, the EU's individuals, businesses, and critical infrastructures are increasingly vulnerable. Recent data from the *European Repository of Cyber Incidents*, visualised in Figure 5, underscores the severity of this trend. In 2023 alone, there were 500 recorded cyberattacks on critical infrastructure, making it the most frequently targeted sector. As of early 2024, 89 incidents had already been reported, suggesting that these threats remain a pressing concern. The graph below illustrates the distribution of political cyberattacks by sector, providing a clear picture of the scale and impact of these threats.

Figure 5: Cybercrime: Critical Infrastructure is Top Target[138]



Source: BLACKSEA CASPIA (2024). The sectors most targeted by cybercrime, *BLACKSEA CASPIA*.

More recent findings from the *ENISA Threat Landscape 2024* further reinforce these concerns. The report recorded 11,079 cyber incidents in the EU between mid-2023 and mid-2024. Of these

[136] *Ibidem.*
[137] *Ibidem.*
[138] BLACKSEA CASPIA (2024). The sectors most targeted by cybercrime, *BLACKSEA CASPIA*.

incidents, 322 attacks affected multiple Member States simultaneously, with energy, finance, and healthcare sectors being the primary targets[139]. Denial-of-service and ransomware attacks remained the most disruptive, threatening essential services and economic stability. The energy sector reported over 200 cyber incidents, with more than half directly impacting EU Member States[140].

This data shows that despite significant regulatory developments and strategic initiatives undertaken over recent years, Europe continues to experience a high volume of cyberattacks, underscoring persistent weaknesses. Examining the evolution of cybersecurity strategies and measures adopted is essential to understanding this ongoing challenge.

2.2.1. The Cybercrime Convention (2001) and Early Directives

The EU's journey in cybersecurity began in the early 2000s with the publication of the 2001 *Cybercrime Convention*[141], which focused on information infrastructure security and the fight against cybercrime. This communication was later complemented by the one on Network and Information Security (NIS), defined as:

> *"Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems."*[142]

The definition provided by the NIS directive is accompanied by a framework that categorises various threats to network security. These threats include communication interception, unauthorised access to computer systems and networks, network disruptions, execution of malicious software that alters or destroys data, identity theft, and environmental incidents or

[139] ENISA (2024). ENISA Threat Landscape 2024, *European Union Agency for Cybersecurity*.
[140] *Ibidem.*
[141] COMMISSIONE EUROPEA, Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica. eEurope 2002 (COM(2000)890), 26 gennaio 2001.
[142] Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment Bruxelles, 6.6.2001 COM(2001)298, p. 10.

unforeseen events[143]. During the same period, the European Union adopted three key directives under the Network and Information Security framework: Directive 2002/21/EC[144], which regulated access and authorisations for electronic communication networks and services; Directive 2002/19/EC[145], which governed access to networks, related resources, and interconnections; and Directive 2002/20/EC[146], which set authorisation requirements for electronic communication networks and services. However, in 2009, these directives were amended with the adoption of Directive 2009/140/EC,[147] which required that Member States implement national measures to strengthen network security and establish dedicated national cybersecurity authorities. Since then, the European Union has increasingly recognised the growing importance of digital infrastructure and has progressively formalised its cybersecurity policies. Initial efforts focused on raising awareness and implementing basic security protocols; however, in the past decade, regulatory activity has intensified, reflecting the increasing complexity and frequency of cyberattacks. This shift became particularly evident following the 2007 Denial-of-Service attacks on Estonia[148], which severely disrupted public institutions and critical infrastructure. Since then, multiple high-profile cyber incidents have exposed the vulnerabilities of European institutions, including attacks on the European Commission, the European Parliament, and the European External Action Service.

2.2.2. ENISA (European Union Agency for Network and Information Security)

A key milestone for European cybersecurity came in 2004 with the establishment of ENISA (European Union Agency for Network and Information Security) through Regulation (EC) No. 460/2004[149]. This agency was tasked with enhancing the resilience of the Union's digital ecosystem by supporting member states and EU institutions in preventing and managing cyber

[143] *Ivi, p.3.*
[144] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) *OJ L 108, 24.4.2002, p. 33–50.*
[145] Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) *OJ L 108, 24.4.2002, p. 7–20.*
[146] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorization of electronic communications networks and services (Authorization Directive) *OJ L 108, 24.4.2002, p. 21-32.*
[147] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC, 2002/19/EC and 2002/20/EC. *OJ L 337, 18.12.2009, p. 37–6.*
[148] Schmidt, A. (2013). The Estonian cyberattacks. In Jason Healey (Cur.), The Fierce Domain – Conflicts in Cyberspace 1986-2012 (pp. 174-193). Washington, D.C.: Atlantic Council.
[149] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) *OJ L 77, 13.3.2004, p. 1–11.*

threats. Its foundation marked the EU's formal recognition of the need for a coordinated, cross-border approach to cybersecurity, particularly in protecting critical infrastructure[150].

As articulated by the agency itself, its mission is *"to achieve a high common level of cybersecurity across the Union"* while acting as *"a centre of expertise on cybersecurity"*[151]. It operates across several key areas to fulfil this mandate, including technical assistance, policy development, capacity building, and awareness raising.

Over the years, ENISA's role has evolved significantly. It was substantially reinforced by adopting the EU Cybersecurity Act (Regulation (EU) 2019/881)[152], discussed later in detail. This act granted the agency a permanent mandate and expanded its responsibilities. It cemented the agency's position as the Union's principal cybersecurity body and introduced the *European Cybersecurity Certification Framework*[153].

Today, ENISA plays a crucial role in safeguarding essential sectors such as energy, healthcare, finance, and transport. It also coordinates large-scale cybersecurity exercises, such as *Cyber Europe,* which simulate complex cyberattack scenarios to assess the resilience of critical infrastructure. These exercises are instrumental in identifying vulnerabilities and strengthening collaborative defence mechanisms, mitigating risks before they translate into real-world consequences. Recognising that different sectors face unique challenges, ENISA has also launched sector-specific initiatives. For instance, it has created guidelines for the energy sector, focusing on the vulnerabilities of smart grids and industrial control systems[154]. In this regard, it has worked closely with the European Commission's NIS Cooperation Group, providing specialized training and situational reports to cybersecurity authorities in the energy industry.

ENISA's stance reflects a commitment to protecting the digital economy and essential public services. The agency has stated that the intention is *"to keep our economy, our society, and our citizens digitally secure"* while promoting *"trust in the connected economy"*[155].

---

[150] Cenetti C. (2014), Cybersecurity: Unione Europea e Italia. Prospettive a confronto, p. 25.
[151] ENISA (2025). A Trusted and Cyber Secure Europe - ENISA Strategy.
[152]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1 *OJ L 151, 7.6.2019, p. 15–69.*
[153] The EU's Cybersecurity Certification Framework for Information and Communication Technology (ICT) products enables tailored and risk-based EU certification schemes. Certification plays a crucial role in increasing trust and security in critical products and services for the digital world. Definition From the official website of the European Union.
[154] Franchina L. - Fulgenzi C. (2024). Cyber Europe 2024, anche l'ACN protagonista per la resilienza dell'infrastruttura energetica. Cybersecurity360.
[155] ENISA (n.d.) 'What we do', *ENISA – European Union Agency for Cybersecurity*.

2.2.3. Safeguarding Critical Infrastructures (EPCIP)

In 2006, the adoption of the *European Programme for Critical Infrastructure Protection* (EPCIP)[156] marked a significant step towards a unified European strategy for safeguarding critical infrastructures. This initiative responded to the Justice and Home Affairs Council's 2005 request for a comprehensive approach to protect essential sectors across member states. It aimed to *"improve the protection of critical infrastructure in the European Union"*[157] through coordinated policies addressing threats from terrorism, crime, natural disasters, and technological failures. The EPCIP defined European Critical Infrastructures as facilities, networks, and services whose disruption would significantly impact public safety, economic stability, or governmental operations. The EPCIP *Action Plan has been launched as part of this initiative* and is structured around three main workstreams. The first is *strategic measures*, horizontal policies applicable across sectors, including risk assessment, mitigation strategies, and capacity building. The second one concerns the *protection of critical European infrastructures,* with targeted efforts to reduce ECI vulnerabilities through regular threat assessments and sector-specific security measures. Lastly, another measure is the *support for national critical infrastructures (NCIs)*; while member states remained responsible for their NCIs, the EU provided guidance and resources to strengthen national strategies[158]. To facilitate real-time threat sharing, the Critical Infrastructure Warning Information Network[159] was established as a secure platform for exchanging best practices and rapid alerts, recognising that disruption within the EU could have cross-border effects. Financially, EPCIP was supported by the Prevention, Preparedness, and Consequence Management of Terrorism and Other Security-Related Risks program from 2007 to 2013, which funded capacity-building projects and technological advancements[160]. However, since 2014, funding for critical infrastructure protection has primarily come from Horizon Europe and the Internal Security Fund[161]. Overall, this program

[156] Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007].
[157] *Ibidem.*
[158] *Ibidem.*
[159] Department of Homeland Security (2010) 'IT Program Assessment: NPPD – Critical Infrastructure Warning Information Network (CWIN).
[160] Council Decision 2007/124/EC of 12 February 2007 establishing for the period 2007 to 2013, as part of the General Programme "Security and Safeguarding Liberties", the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks".
[161] European Commission (2024) Critical infrastructure resilience at EU-level, *Official Website of the European Union.*

laid the groundwork for subsequent EU cybersecurity frameworks, including the NIS Directive (2016) and the Critical Entities Resilience (CER) Directive (2022).

2.2.4. NIS (2016) Directive

As mentioned, the first horizontal EU legislation to address cybersecurity challenges and revolutionise European resilience and cooperation was the Directive on the Security of Network and Information Systems (NIS, Directive EU No. 2016/1148)[162]. Adopted in July 2016, it established a common framework to enhance the resilience of critical infrastructure across member states. According to the European Commission, the directive aimed to *"achieve a high common level of security of network and information systems within the Union"*[163] by strengthening national capabilities, fostering cooperation, and promoting risk management practices among key economic actors.

The NIS Directive targeted societal and economic well-being sectors, including energy, transport, banking, financial markets, healthcare, water supply, and digital infrastructure. Entities within these sectors were classified into two primary categories: *Operators of Essential Services* and *Digital Service Providers*. Both categories were required to implement appropriate security measures and report significant incidents to national authorities[164]. Following the approval of the Directive, each European nation began drafting national laws to define strategic objectives and enforcement measures. States had a certain degree of flexibility to adapt to national circumstances, such as the ability to reuse existing organisational structures or align with pre-existing national legislation. Each state had to establish one or more *Computer Security Incident Response Teams*[165] and designate competent authorities to oversee compliance. Lastly, the adoption of the NIS Directive expanded ENISA's role. Previously focused on promoting best practices and providing technical guidance, its mandate was strengthened to include direct support for member states in managing cyber risks and facilitating stakeholder cooperation [166].

---

[162]Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30*

[163] *Ibidem.*

[164] *Ibidem.*

[165] A group of experts that assesses, documents and responds to a cyber incident so that a network can recover quickly and avoid future incidents.

[166]ENISA (2016).ENISA's Position on the NIS Directive. Version 1.0.

In 2017, the Trusted Information Security Assessment Exchange (TISAX) was established as a globally recognised framework for information security assessments, particularly within the automotive industry. Initially developed by the German Association of the Automotive Industry (VDA), TISAX ensures that companies across the supply chain adhere to consistent cybersecurity standards. While not an EU-led initiative, its adoption across Europe reflects the broader trend toward harmonised security practices within critical industries[167].

2.2.5. From the EU Cybersecurity Act to NIS2

A more comprehensive step toward a unified cybersecurity strategy came with the adoption of the EU Cybersecurity Act in 2019 (Regulation (EU) 2019/881)[168]. This act comprises two key pillars. The first focuses on ENISA's enhanced role, expanding its responsibilities beyond technical advisory functions to more active support for incident management. The second pillar introduces a European cybersecurity certification framework[169], designed to establish common standards for ICT products, services, and processes across member states. As the European Commission stated, *"the absence of mutual recognition among existing national certification schemes created fragmentation, undermining cross-border operations within the digital single market"*[170]. The Cybersecurity Act addresses this challenge by creating a framework that ensures that certifications issued under EU schemes are recognised across all member states.

Despite these advancements and the fact that the NIS Directive represented a significant milestone in the EU's approach to cybersecurity, its implementation revealed challenges. Variations in how member states transposed the directive into national law led to inconsistencies in incident reporting, risk assessment, and enforcement practices across the Union. According to the European Commission, *"the directive's implementation revealed fragmentation, with residual low cyber resilience among businesses and varying levels of preparedness across sectors"*[171]. Moreover, the growing complexity and frequency of cyberattacks, alongside the increasing

[167] Pravitz S. (2021). "Das Wichtigste zum Tisax-Update". *Automobil Industrie*.
[168] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing. Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1 *OJ L 151, 7.6.2019, p. 15–69*
[169] *Ibidem.*
[170] European Commission (2017). REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").
[171] Negreiro, M. (2021) *The NIS2 Directive: A high common level of cybersecurity in the EU*. European Parliamentary Research Service.

digitalisation of critical infrastructures, highlighted the need for a more robust and harmonised framework.

This led to adopting the NIS2 Directive in 2022 (Directive (EU) 2022/2555)[172], which introduced a more comprehensive cybersecurity framework and ensured that the measures kept pace with evolving threats. One of the most notable advancements is its expanded scope. While the original NIS Directive focused on a limited set of critical sectors, NIS2 broadened its application to both *"essential entities"* and *"important entities",* based on the significance of the services provided[173]. This expansion encompasses a broader range of industries, including energy, transport, banking, financial market infrastructures, healthcare, drinking water supply and distribution, digital infrastructure, public administration, and space (NIS2 Directive, Art. 2)[174]. This broader scope reflects the EU's recognition of the interconnected nature of modern economies, where disruptions in one sector can trigger cascading effects across multiple domains. Additionally, it eliminates the previous threshold-based approach for determining obligations. Instead, entities are now classified based on the criticality of their services rather than solely on their size. As ENISA emphasises, the revised scope ensures that medium-sized and large entities in critical sectors adhere to the same baseline security requirements[175] regardless of their market share.

The NIS2 Directive introduces several critical obligations for covered entities to strengthen cyber resilience. One of the most significant is the implementation of risk management measures, requiring both essential and vital entities to establish comprehensive cybersecurity risk management frameworks. As stated in the directive, *"entities shall take appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of network and information systems"* (NIS2 Directive, Art. 21)[176]. Another fundamental obligation is incident reporting, with the directive imposing stricter requirements. Entities must notify national authorities or CSIRTs of significant cyber incidents within 24 hours of detection, followed by an intermediate report within 72 hours and a final report within one

[172] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (OJ L 333 27.12.2022, p. 80).

[173] *Ibidem.*

[174] Directive (EU) 2022/2555, Art. 2.

[175] European Union Agency for Cybersecurity (ENISA), 2023. *Good Practices for Supply Chain Cybersecurity*. [pdf] Available at: https://www.enisa.europa.eu/.

[176] Directive (EU) 2022/2555, Art. 21.

month. These requirements ensure rapid response coordination and enhanced mitigation efforts across borders (NIS2 Directive, Art. 23)[177].

Recognising the heightened risks complex supply chains pose, the directive mandates stronger supply chain security measures. Entities must assess and manage cybersecurity risks associated with third-party suppliers, ensuring that vendors adhere to the same security standards. This approach reinforces the resilience of the broader digital ecosystem. Furthermore, the directive establishes requirements for vulnerability disclosure and patch management to minimise cyber risks. Entities must develop coordinated vulnerability disclosure policies and implement prompt security updates. This provision ensures that known vulnerabilities are addressed swiftly, minimising the risk of exploitation[178].

Governance and accountability are also central elements of NIS2. The directive places greater responsibility on senior management, requiring them to oversee cybersecurity risk management measures within their organisations. Leadership must actively ensure compliance and risk awareness throughout the entity. As the directive states, *"management bodies of essential and important entities shall approve the cybersecurity risk-management measures taken by the entity and supervise its implementation"* (NIS2 Directive, Art. 20)[179].

To promote a coordinated response to cyber threats, NIS2 also establishes the European Cyber Crises Liaison Organisation Network, which facilitates the joint management of large-scale cybersecurity incidents and crises (NIS2 Directive, Art. 15)[180]. Entities are further encouraged to exchange best practices, threat intelligence, and mitigation strategies while ensuring the protection of sensitive information.

Enforcement mechanisms and penalties have also been strengthened under NIS2. The deadline for transposition into national law was October 2024, requiring all Member States to align their national cybersecurity frameworks with the directive. National authorities are empowered to conduct audits, request compliance documentation, and impose financial penalties for non-compliance. Under the directive, fines can reach €10 million or 2% of an essential entity's global annual turnover and up to €7 million or 1.4% for important entities (NIS2 Directive, Art.

[177] Directive (EU) 2022/2555, Art. 23.
[178] European Commission, (2025). *Security of the supply chain*. [online] Joint Research Centre.
[179] Directive (EU) 2022/2555, Art. 20.
[180] Directive (EU) 2022/2555, Art. 15.

31[181]). To support effective implementation, ENISA is central in offering technical expertise, training, and best practice recommendations to apply NIS2 measures across the EU consistently.

The Cyber Resilience Act (CRA) of 2024[182], adopted by the European Parliament on October 10, 2024, represents another significant step in the EU's harmonisation process. The regulation mandates manufacturers integrate security measures at the design stage rather than relying on post-market fixes. Covering all digital products, from consumer devices to industrial control systems and medical equipment, the CRA establishes strict cybersecurity standards to reduce systemic vulnerabilities, enhance resilience, and strengthen digital security.

A core principle of the CRA is *security by design*[183], requiring manufacturers to embed cybersecurity features during development rather than applying patches after vulnerabilities emerge. Its adoption carries far-reaching implications for businesses, regulators, and consumers. Companies must now adhere to stringent security requirements, with non-compliance resulting in sanctions, including market bans, product recalls, or financial penalties. While compliance may pose initial costs, particularly for SMEs, the long-term benefits include enhanced security, reduced cyber risk, and increased consumer trust. The regulation also streamlines cybersecurity laws by replacing fragmented national rules with a unified framework, reducing administrative burdens and facilitating cross-border business operations. For consumers, the CRA ensures that products are secure by default, lowering the risks of ransomware, data breaches, and unauthorised access. The CRA complements the EU's broader cybersecurity framework. It aligns with the NIS2 Directive, which strengthens cybersecurity requirements for essential services and critical infrastructure, and DORA, which focuses on the financial sector. The Cyber Resilience Act marks a strategic shift in the EU's approach, moving from reactive cybersecurity measures to a preventive strategy that embeds security across the entire product lifecycle[184]. As cyber threats evolve, it is a key instrument in safeguarding Europe's digital infrastructure, reinforcing the EU's leadership in cybersecurity governance, and shaping global cybersecurity regulations.

The European Union has continued to expand its cybersecurity strategy, introducing additional measures in 2025 to strengthen collective defences. A significant development in this regard is

[181] Directive (EU) 2022/2555, Art. 31.
[182] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance) PE/100/2023/REV/1 *OJ L, 2024/2847, 20.11.2024,*
[183] *Ibidem.*
[184] *Ibidem.*

the Cyber Solidarity Act (Regulation (EU) 2025/38)[185], adopted on December 19, 2024, and entered into force on February 4, 2025. One of its key innovations is the European Cybersecurity Alert System, a network comprising National and Cross-Border Cyber Hubs. It utilises advanced technologies like artificial intelligence (AI) and data analytics to detect and respond to cyber threats. Additionally, it facilitates timely cross-border information sharing. By institutionalising these mechanisms, the EU aims to limit the impact of cyberattacks on essential services, public institutions, and economic stability[186].

The EU's cybersecurity approach has evolved significantly over the past two decades, transitioning from individual national efforts to an integrated regulatory framework. There has been a shift from reactive policies to a proactive, risk-based strategy emphasising prevention, resilience, and international coordination. The introduction of mandatory security requirements for digital products, real-time response mechanisms, and collaborative cybersecurity initiatives underscores the EU's long-term commitment to securing its digital ecosystem. The legislative measures introduced in 2024 and 2025 reflect the EU's ambition to maintain the forefront of cybersecurity governance. Establishing structured policies, harmonised security standards, and collective defence mechanisms ensures that Europe is better prepared for cyber challenges.

2.3. NATO's Cybersecurity Policy and Crisis Response Mechanisms

While the European Union focuses on regulatory frameworks to secure critical infrastructure, NATO plays a complementary role by emphasising strategic defence and collective security. The EU primarily seeks to enhance internal resilience among member states through legal and institutional measures. In contrast, NATO adopts a geopolitical approach rooted in allied cooperation and collective defence, particularly in response to cyber threats with geopolitical implications. This section examines NATO's evolving role in managing and mitigating cyberattacks on critical infrastructure, tracing its transformation from initial recognition to comprehensive policy implementation, specifically focusing on the implications of Article 5 of the North Atlantic Treaty.

[185] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) PE/94/2024/REV/1 OJ L, 2025/38, 15.1.2025.
[186] *Ibidem.*

The North Atlantic Treaty Organization is one of the most prominent examples of the ability of international organisations to evolve and adapt over time. This organisation was officially established with the signing of the North Atlantic Treaty on April 4, 1949, which was ratified by ten European states, along with the United States and Canada. Today, NATO comprises 32 member countries, all of which have ratified the treaty and are committed to maintaining interstate security and addressing the urgent challenge of terrorism in all its forms[187]. NATO's ability to adapt to emerging threats depends on the flexibility of its rules, procedures, and strategic objectives, as well as the extent to which its security framework aligns with the evolving challenges faced by its member states[188]. While traditionally perceived as a military alliance centred on collective defence, NATO has developed into a broader international organisation rooted in liberal-democratic values and cooperative security mechanisms. Over time, its role has expanded beyond conventional military deterrence to encompass political and strategic coordination in areas such as cybersecurity[189]. This change underscores NATO's commitment to safeguarding member states from direct military aggression and systemic threats, including cyberattacks on critical infrastructure. NATO has, therefore, the task to enhance trust among allies and mitigate risks through proactive crisis response strategies[190].

Recognising the growing importance of cyber resilience, NATO has progressively transitioned from an ad hoc response to a structured cyber defence policy. This evolution culminated in the explicit recognition of cyberspace as a domain of operations and the acknowledgement that Article 5 of the North Atlantic Treaty may be invoked in response to severe cyberattacks. As NATO has stated, *"A severe cyberattack could lead to the invocation of Article 5, as decided on a case-by-case basis by the North Atlantic Council"*[191]. This adaptation highlights the need for increasing focus on deterrence, resilience, and crisis response in the digital era.

2.3.1. Towards NATO Cyber Defence Programme

NATO's cybersecurity agenda began taking shape in the early 2000s, as digital networks became integral to military operations and civilian infrastructure. The rapid expansion of internet

[187] NATO Official Website. (2020). A short history of NATO.
[188] Wallander, C. A. (2000). Institutional assets and adaptability: NATO after the Cold War. International organization, 705-735.
[189] *Ibidem.*
[190] NATO Official Website. (2020).What is NATO?.
[191] NATO (2023). Collective Defence and Article 5. North Atlantic Treaty Organization Official Website.

technologies exposed vulnerabilities in national defence systems, compelling to reassess the implications of cyber threats for collective security[192]. While cyberattacks were initially viewed as tools for espionage and disruption rather than acts of war, concerns grew about their potential to destabilise economies, communications, and energy infrastructure. The turning point came at the 2002 Prague Summit[193], where NATO members formally committed to strengthening cyber defence capabilities. As the declaration stated, *"NATO will continue to adapt to new threats and challenges, including those posed by cyberattacks, which can undermine the security of Allied nations"*[194]. Cyber threats had not yet significantly impacted its military operations during this period. However, experts within the Alliance warned that hostile actors could exploit digital vulnerabilities to target critical infrastructures such as power grids, banking systems, and communication networks. This realisation marked the beginning of NATO's strategic shift, ultimately redefining cybersecurity as a core pillar of collective defence.

Between 2003 and 2006, the Alliance enhanced collaboration with national cybersecurity agencies and intelligence bodies, conducting initial assessments of how cyber threats could disrupt military operations and compromise national security. The NATO *Cyber Defence Programme*, introduced in 2004, represented one of the first initiatives to develop a structured approach to cyber threats. However, its scope remained limited primarily to internal network protection and information security protocols[195].

2.3.2. The aftermath of Russian DDoS attacks towards Estonia

A significant shift in NATO's regulatory framework came in 2007, when Estonia, a NATO member since 2004, experienced a massive wave of cyberattacks targeting government institutions, banks, media outlets, and infrastructure providers. These attacks, which began in April and lasted for several weeks, slowed essential services and exposed the vulnerabilities of digital infrastructure. The cyberattack disrupted government communications, prevented access to banking services, and paralysed news agencies, revealing the destructive potential of

[192] Pfannenstiel M. - Cox D.(2024).NATO's Cyber Era (1999–2024) Implications for Multidomain Operations. MILITARY REVIEW ONLINE EXCLUSIVE.
[193] *Ibidem.*
[194] Prague Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002.
[195] Pfannenstiel M. - Cox D.(2024).NATO's Cyber Era (1999–2024) Implications for Multidomain Operations. MILITARY REVIEW ONLINE EXCLUSIVE .

coordinated cyber operations. The attacks were widely attributed to Russian state-sponsored actors, particularly in the context of rising geopolitical tensions following Estonia's decision to relocate the Soviet-era Bronze Soldier of Tallinn war memorial. Although Moscow denied involvement, cybersecurity experts and intelligence agencies identified clear signs of an orchestrated campaign involving distributed denial-of-service attacks that overwhelmed Estonia's digital networks[196]. The Estonian government described the incident as *"the first cyberwar in history,"*[197] making it the first instance in which a formal request for assistance was issued following a cyberattack. This event, however, exposed the lack of a coordinated international response mechanism for large-scale cyber incidents[198]. As NATO's CCDCOE later reported, *"an attack on a member state's digital infrastructure can have significant implications for its national security and, by extension, for the Alliance"*[199].

In the aftermath of this attack, NATO took significant steps to shape its cyber policy framework, demonstrating a swift and proactive response to cyber defence challenges. It implemented a provisional set of tools to help its members counter future cyberattacks. While the task remained complex and demanding, most member states had always expressed confidence in the measures adopted by the Alliance.

Cyber defence became an independent pillar of the organisation's activities. NATO had laid two key foundations in developing its *"Cyber Defence 1.0"* framework. First, it established the *Cyber Defence Management Authority* to oversee cybersecurity initiatives. Additionally, it created an intellectual platform for long-term doctrinal and strategic thinking on cyber operations through the foundation of the Cooperative Cyber Defence Centre of Excellence (CCDCOE)[200]. The CCDCOE, formally established on May 14, 2008, became operational on October 28, 2008, acquiring the status of an international military organisation. It is regarded as one of NATO's most advanced cyber defence institutions today. A multinational, interdisciplinary hub that enhances cyber resilience by focusing on research, training, and policy development. Its mission is to provide member states with expertise in cybersecurity technology, strategy, and law, assisting them in strengthening their national defences against cyber threats[201]. Initially, only

[196]Schmidt, A. (2013). The Estonian cyberattacks. In Jason Healey (Cur.), The Fierce Domain – Conflicts in Cyberspace 1986-2012 (pp. 174-193). Washington, D.C.: Atlantic Council.
[197] McGuinness D. (2017). How a cyber attack transformed Estonia. BBC News.
[198] Hughes, R. (2009). NATO and Cyber Defence. Atlantisch Perspectief, 33.
[199] Burton, J. (2015) NATO's cyber defence: Strategic challenges and institutional adaptation. Defence Studies. 15 (4), 297-319.
[200] NATO Allied Command Transformation (2023). *NATO Centres of Excellence – Cooperative Cyber Defence (CCD COE).*
[201]*Ibidem.*

seven nations formally signed its founding agreement, but as of 2025, the Centre includes 39 participating nations and employs cybersecurity experts from these countries. Although full membership is available exclusively to NATO Allies, non-member states may join as contributing participants.

One of the most significant contributions of the CCDCOE has been the development of *Locked Shields*, an annual live-fire cyber defence exercise widely regarded as one of the world's largest and most complex cyber defence drills. These exercises simulate large-scale cyberattacks on critical infrastructure, testing and refining NATO's response capabilities. Participants engage in real-time threat mitigation scenarios, developing essential skills for countering cyber incidents[202]. As the CCDCOE emphasised, *"The exercise not only enhances technical cybersecurity skills but also strengthens strategic decision-making and cooperation among allied nations"*[203].

Beyond training exercises, it has developed international legal frameworks for cyber warfare. The Centre spearheaded the creation of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2005). This groundbreaking legal study examines how existing international law applies to cyber conflicts. This manual has since become a foundational reference for policymakers and military strategists worldwide, helping establish normative standards for responsible state behaviour in cyberspace[204].

The second major initiative after the attack came in 2016, during the Warsaw Summit when NATO formalised its commitment to cyber defence by adopting the Cyber Defence Pledge[205]. This pledge acknowledged the cyber domain as the fifth operational domain alongside land, sea, and air. It required member states to allocate additional resources to strengthen national cybersecurity defences, although no specific minimum investment was mandated[206]. This decision represented a fundamental shift in NATO's strategic posture, as the Alliance affirmed that "*the ability to operate effectively in cyberspace is essential to NATO's core tasks of collective defence, crisis management, and cooperative security."*[207] An effective cyber defence strategy ultimately fosters a trust-based community where information and technological

[202] NATO Cooperative Cyber Defence Centre of Excellence, 2025. *Locked Shields*. [online] Available at: https://ccdcoe.org/locked-shields/.
[203] *Ibidem.*
[204] NATO Cooperative Cyber Defence Centre of Excellence, 2025. *The Tallinn Manual*. [online] Available at: https://ccdcoe.org/research/tallinn-manual/.
[205] NATO. (2016) Cyber Defence Pledge. North Atlantic Treaty Organization.
[206] Shea, J. (2017). How is NATO meeting the challenge of cyberspace?. Prism, 7(2), 18-29.
[207]NATO, 2024. *Cyber defence*. [online] Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm

advancements are shared, ensuring that no member state becomes a weak link in the broader security framework.

2.3.3. Article 5 of the North Atlantic Treaty Organization and its Implications

The principle of collective defence, established with the signing of the North Atlantic Treaty in 1949, remains the central pillar of NATO and has been the subject of extensive debate. This principle is unique because it creates a binding commitment among all member states, requiring them to collaborate in the event of an attack against one of them[208]. Article 5 of the treaty explicitly states that if a NATO ally becomes the target of an armed attack, the alliance's other members must consider the aggression as an attack against the entire organisation. They must take all necessary actions to defend the affected state. Article 5 of the Treaty officially declares:

> *"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.*
>
> *Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."*[209]

Although Article 5 has been formally invoked only once, it remains the most significant deterrent against external aggression from state or non-state actors.

Since the alliance's founding, the nature of warfare has evolved significantly, expanding NATO's strategic considerations to include cyberspace as a key defence area. This shift has been driven by the increasing recognition that cyber threats pose substantial risks to national security, with

[208]NATO (2023). Collective Defence and Article 5. North Atlantic Treaty Organization Official Website.

[209] Yale Law School, Lillian Goldman Law Library, n.d. *The North Atlantic Treaty; April 4, 1949*. [online] The Avalon Project. Available at: https://avalon.law.yale.edu/20th_century/nato.asp.

the potential to cause severe disruptions even in the absence of physical destruction. The Deputy Assistant Secretary of Defence for Cyber Policy, Aaron Hughes, has emphasised that cyber threats require a resolute and strategic response, given that cyberspace has become an essential operational domain in modern conflict.[210]

In response to these evolving security challenges, NATO heads of state and government convened on September 5, 2014. They issued the Wales Declaration, marking a critical turning point in the alliance's cyber defence policy. This declaration formally recognised cyber threats as a growing and urgent security issue, outlining the strategic approach based on prevention, detection, resilience, recovery, and defence [211]. Additionally, it established that international law, including the laws of armed conflict and the United Nations Charter, applies equally to cyber operations, reinforcing the principle that states must adhere to international legal norms in cyberspace[212]. The Wales Declaration explicitly confirmed that Article 5 extends to cyberattacks, with the North Atlantic Council determining on a case-by-case basis whether a cyber incident constitutes grounds for collective defence action.[213]

However, like any other international treaty, the North Atlantic Treaty is inherently shaped by the historical context in which it was signed. Consequently, it is unsurprising that it contains no explicit references to the cyber domain. Although NATO has continued to employ the explicit language of Article 5 to regulate all aspects of armed attacks, cyberattacks present unique and unprecedented challenges. As analysed previously in this thesis, cyberattacks differ significantly in identifying characteristics from traditional models of dynamic warfare. Unlike conventional attacks, which typically cause immediate and visible destruction, cyberattacks have the potential to devastate a nation without producing initial physical damage. This distinction underscores the difficulty of mounting an effective and timely defensive response, given the need for immediacy[214]. Article 5 is insightful in assessing actions undertaken by state and non-state actors in conventional warfare. However, NATO allies drafted it considering the technologies and strategies used after World War II. This implies that legitimately invoking Article 5 as a response

[210] Aaron Hughes, Deputy Assistant Secretary of Defence. (2016). Statement on Digital Acts of War: Evolving the Cybersecurity Conversation, Before the H. Comm. on Oversight and Government Reform Subcomms. on Information Security and National Security, 114th Cong. 1.

[211] NATO. (2018). Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.

[212] *Ibidem.*

[213] NATO. (2015). Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar.

[214] Jackson S. (2016). NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack. The CIP Report.

to cyberattacks depends on the Alliance's ability to define a clear and unified standard for what constitutes an armed attack, thereby allowing cyberattacks to be treated as such under its provisions. The absence of a uniform definition would inevitably lead to debate among allied states over any response against an attack on a member state. This issue is further compounded by the Wales Summit Declaration, which explicitly states that each attack must be assessed on a case-by-case basis.[215]

The most significant concepts regarding cyber defence are outlined in paragraphs 72 and 73 of the Declaration. This declaration marked NATO's first significant and groundbreaking shift in cybersecurity policy. Before this moment, despite multiple cyberattacks, such as those targeting Estonia (2007), the United States (2008), and Georgia (2008)[216], no international organisation had ever provided such a clear and explicit stance on the matter. Paragraph 72 acknowledges that cyber threats and attacks will continue to become more frequent, increasingly sophisticated, and capable of causing greater harm[217]. Any remaining uncertainty regarding cyberattacks is further clarified at the end of the same paragraph, where it is explicitly stated that:

> *"Cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."*[218]

Based on this, paragraph 73 establishes that a fundamental task of the Alliance will be to develop national cyber defence capabilities further, and enhance the cybersecurity of national networks on which NATO's operations depend. It will also promote the exchange of information as much as possible. This will include increasing situational awareness among allies.[219]

Furthermore, through the Wales Declaration, it commits to exchanging and sharing information with other international organisations, whether global or regional, such as its ongoing

[215] *Ibidem.*
[216] Swanson L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 russian-georgian cyber conflict. Loyola of Los Angeles International and Comparative Law Review, 32(2), 303-334.
[217] NATO. (2018). Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.
[218] *Ibidem.*
[219] *Ibidem.*

cooperation with the European Union. It also aims to strengthen collaboration with the private sector, recognising this as one of the most effective methods for reinforcing cybersecurity defences. Additionally, NATO pledges to facilitate knowledge-sharing with individuals through education, training, and cyber defence exercise programs.

Following the adoption of the Wales Declaration, two key observations emerged that merit further analysis. As highlighted by Polish diplomat and government official Grzegorz Kostrzewa Zorbas, NATO needed to fully, swiftly, and precisely integrate the issues of cyber warfare, cyber defence, and cyber weapons[220]. In response, NATO has undertaken significant steps to enhance its cyber defence posture. In 2016, it recognised cyberspace as a domain of operations, placing it alongside traditional domains such as air, land, and sea. This recognition enabled NATO's military commanders to better protect missions and operations from cyber threats by drawing on Allies' national cyber capabilities[221]. The second observation concerns establishing a dedicated Cyber Command to enhance its ability to respond to cyber threats with greater coordination and operational efficiency. In this regard, in 2018, NATO defence ministers launched the Cyber Operations Centre (CyOC) at Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium[222]. It was designed as a central hub for monitoring, assessing, and countering cyber threats targeting NATO networks and critical infrastructure. Its primary mission is to enhance situational awareness in cyberspace, fortify its cyber defence posture, and integrate cyber capabilities into the Alliance's broader military strategy. At the time of its launch, it emphasised its crucial role, stating: *"The Cyber Operations Centre ensures that NATO can respond effectively to cyber incidents, strengthening the protection of critical infrastructure."*[223] A key function is to provide NATO commanders with real-time cyber intelligence, allowing for informed decision-making during military operations. Incorporating cyber awareness into strategic planning ensures that digital threats are assessed alongside conventional security challenges. To enhance its effectiveness, the CyOC continuously expands its capabilities by integrating artificial intelligence and machine learning technologies to improve threat detection and automate response mechanisms. These advancements identify cyber threats with greater

[220] Kostrzewa-Zorbas, G. (2014). NATO in the new strategic environment: Cyberattacks now Covered by article 5 of the north atlantic Treaty. Studia Bezpieczeństwa Narodowego, 4(6), 397-418.
[221] NATO Cooperative Cyber Defence Centre of Excellence, 2016. *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*.
[222] NATO Supreme Headquarters Allied Powers Europe (SHAPE), n.d. *Cyber Defence*. [online] Available at: https://shape.nato.int/about/aco-capabilities2/cyber-defence
[223] NATO Rapid Deployable Corps Italy, n.d. *NATO Cyber Operation Centre.*

speed and precision, reducing the likelihood of large-scale cyber incidents affecting military and civilian infrastructure.

2.3.5. Advancements in NATO's Cybersecurity Policies for Protecting Critical Infrastructures

In 2019, NATO launched the Cyber Rapid Reaction Teams, specialised units designed to provide immediate assistance to member states facing major cyber incidents. These teams are tasked with detecting, analysing, and mitigating cyber threats in real time, preventing disruptions to critical infrastructure, military networks, and government systems. Providing hands-on support and expertise reinforces collective cyber resilience.[224]

A key function of the CRRTs is active cyber threat hunting, where teams proactively search for indicators of compromise (IoCs) within their networks. This preemptive approach enhances its defences by identifying and neutralising threats before they escalate into full-scale incidents. Additionally, CRRTs conduct penetration testing and vulnerability assessments, evaluating national cyber infrastructures and recommending improvements to mitigate risks. These teams work in close coordination with other NATO cybersecurity entities, including the Cyber Operations Centre, the NATO Computer Incident Response Capability (NCIRC), and the Cooperative Cyber Defence Centre of Excellence.[225] This integrated approach ensures a swift, efficient, and coordinated response to cyber crises while strengthening NATO's long-term cyber resilience.

Recognising that cyber defence extends beyond military structures, NATO adopted the 2021 Comprehensive Cyber Defence Policy, emphasising closer collaboration between military and civilian cybersecurity entities. The policy acknowledged that critical sectors such as energy, finance, healthcare, and transportation had become primary targets for cyber adversaries. To address these vulnerabilities, NATO promoted deeper cooperation with industries, cybersecurity firms, and research institutions, fostering the development of cutting-edge technological solutions and enhancing cyber defence interoperability across the Alliance.[226]

---

[224]Pfannenstiel M. - Cox D.(2024).NATO's Cyber Era (1999–2024) Implications for Multidomain Operations. MILITARY REVIEW ONLINE EXCLUSIVE.

[225] *Ibidem.*

[226] *Ibidem.*

Between 2021 and 2024, NATO significantly expanded its cyber defence capabilities, integrating AI-driven cybersecurity solutions, automated threat detection systems, and quantum-resistant encryption protocols. These technological advancements were critical as adversaries increasingly leveraged AI-powered cyberattacks, deepfake disinformation campaigns, and hybrid warfare tactics to undermine democratic institutions and military decision-making processes. By incorporating AI and automation, NATO improved its ability to detect and neutralise cyber threats quickly and accurately, minimising the risk of large-scale digital disruptions.[227]

As cyber threats evolved, it expanded its focus to maritime cybersecurity, particularly protecting undersea infrastructure such as submarine communication cables and offshore energy installations. These assets are critical to its strategic and economic stability, as they facilitate global internet connectivity, energy distribution, and secure military communications. Amid rising concerns over state-sponsored sabotage and cyber-enabled physical attacks on maritime infrastructure, NATO integrated autonomous naval drones equipped with AI-driven threat detection systems. These autonomous surveillance systems patrol and monitor critical undersea zones, enhancing NATO's ability to detect and respond to suspicious activities in real-time.[228]

In 2025, it expanded the scope of its Cyber Rapid Reaction Teams (CRRTs) to cover a broader range of advanced cyber threats, including Advanced Persistent Threats (APTs). These teams were further embedded within NATO's broader multi-domain defence strategy, ensuring that cyber defence seamlessly integrates with land, air, sea, and space operations. During a briefing in 2025, Alliance leaders reiterated that in today's interconnected world, cyber defence is not just a military concern; it is an economic and societal imperative.

Despite NATO's substantial investments in cybersecurity, cyberattacks on critical infrastructure continue to rise, highlighting digital threats' persistent and evolving nature. Between January 2023 and January 2024, *"critical infrastructure worldwide sustained over 420 million attacks, equivalent to 13 attacks per second, marking a 30% increase from 2022."*[229] This dramatic increase reflects an evolving threat landscape in which state-sponsored and criminal actors systematically exploit digital vulnerabilities to cause widespread disruption. The United States alone reported a 70% rise in cyberattacks on utility providers in 2024, largely attributable to the

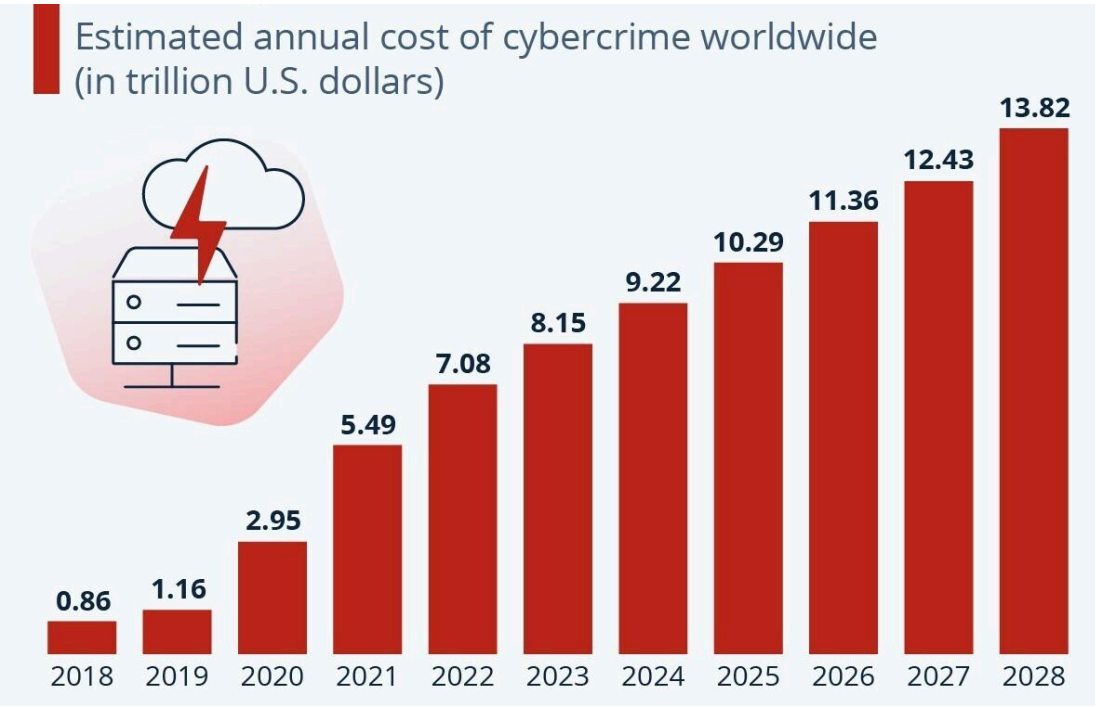
[227] *Ibidem.*
[228] McNamara, E.M., 2024. Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure. [online] NATO Review.
[229] KnowBe4, (2024). *KnowBe4 Report Reveals Critical Infrastructure Under Siege with Cyber Attacks Increasing 30 Percent in One Year*.

digital expansion of the power grid and its attendant security vulnerabilities[230]. This cyberattack escalation transcends national concerns, directly impacting NATO's capacity to maintain collective security across its alliance. In 2024, Microsoft reported that cyberattacks against critical infrastructure had doubled, with 40% of all nation-state cyber operations targeting essential services.[231] Much of this activity has been linked to geopolitical tensions, particularly Russian cyber operations against Ukraine and NATO allies. According to the U.S. Cybersecurity and Infrastructure Security Agency, *"Russian military cyber actors have actively targeted government, transportation, financial, and healthcare sectors across at least 26 NATO members"*[232]. Concurrently, Chinese-backed hackers have been implicated in infiltrating British parliamentary networks and voter databases, highlighting the strategic nature of these digital offensives in achieving geopolitical objectives.[233]

Beyond their immediate security implications, cyberattacks on critical infrastructure carry significant economic consequences. The global financial toll of cyber incidents doubled in 2024 compared to the previous year, with projected costs exceeding $1 trillion in the event of a significant attack on the U.S. power grid[234]. The following graph (Figure 6) illustrates the alarming upward trend in the financial cost of cybercrime worldwide. The economic impact of cyberattacks has surged from $0.86 trillion in 2018 to a projected $13.82 trillion by 2028, illustrating the urgent need for stronger cybersecurity frameworks across NATO member states.

[230] Dareen S. - Srivastava V. (2024). Cyberattacks on US utilities surged 70% this year, says Check Point. Reuters.
[231] Microsoft Corporation, (2024). *Microsoft Digital Defence Report 2024*.
[232] Cybersecurity and Infrastructure Security Agency, (2024). *Russian Military Cyber Actors Target US and Global Critical Infrastructure*.
[233]Gregory J. - Watson I. (2024). China linked to UK cyber-attacks on voter data, Dowden to say. BBC.
[234] Allianz Commercial, 2024. *Allianz Risk Barometer 2024 - Cyber incidents*.

Figure 6: Cybercrime Expected to Skyrocket[235]



Source: Fleck, A. (2024). Cybercrime Expected To Skyrocket in Coming Years. [online] EBnet.

Concluding, an IR constructivist perspective provides a valuable theoretical framework for understanding NATO's evolving stance on cybersecurity. Constructivism argues that material threats do not solely determine security but are also shaped by perceptions, identities, and normative frameworks among international actors.[236] NATO's historical focus on conventional warfare and deterrence initially limited its engagement with cybersecurity. However, as cyberattacks grew in scale and sophistication, NATO began perceiving cyberspace as integral to its collective security identity, framing cyberattacks not merely as technical disruptions but as existential threats to state sovereignty[237]. This shift was evident when the 2014 Wales Summit Declaration formally recognised that cyberattacks could trigger Article 5, marking a transformative moment in its conceptualisation of security. NATO's cybersecurity policies

[235] Fleck, A. (2024). Cybercrime Expected To Skyrocket in Coming Years. [online] EBnet.
[236] Eriksson J. - Giacomello G. (2014). International Relations, Cybersecurity, and Content Analysis: A Constructivist Approach. The Global Politics of Science and Technology - Vol. 2 (pp.205-219) Chapter 6.
[237] Dunn Cavelty M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge.

evolved not merely in response to material threats but also through changing strategic narratives that redefined cyber threats as central to its deterrence and defence strategy. This shift stresses Constructivism's central argument: security is not static but socially constructed through shared norms, experiences, and institutional learning.

However, from a realist perspective, NATO's increasing focus on cybersecurity reflects a response to the growing material capabilities of adversaries and the anarchic nature of the international system. Realism contends that states and alliances prioritise security based on tangible power dynamics, where cyber capabilities represent a new frontier for power projection and coercion. The integration of cybersecurity into NATO's strategic framework can thus be seen as a rational adaptation to technological advancements and the cyber capabilities of rival states such as Russia and China. While constructivists emphasise identity and norms in shaping NATO's response, realists would argue that these shifts are ultimately driven by the imperative to maintain military superiority and strategic deterrence. The recognition of cyberattacks as potential triggers for Article 5 underscores NATO's commitment to upholding credible deterrence, reinforcing realism's claim that security policies are dictated by power considerations and the necessity to counter emerging threats. Thus, while constructivism explains the evolving narratives around cybersecurity, realism highlights the material power struggles that ultimately shape NATO's strategic decisions.

2.4. EU and NATO Strategic Partnership

The strategic partnership between the European Union and the North Atlantic Treaty Organization is fundamental to ensuring security and stability across the Euro-Atlantic region. Rooted in shared values and mutual commitments to peace, freedom, and prosperity, this collaboration acknowledges that modern security threats, particularly cyberspace, demand coordinated responses. Over the years, EU-NATO cooperation has grown increasingly indispensable as both organisations work together to protect critical infrastructures from cyber threats, hybrid warfare, and geopolitical risks.

The formalisation of EU-NATO relations dates back to the early 2000s, building upon initiatives developed in the 1990s to promote greater European responsibility in defence. NATO has historically been the foundation of collective defence for its members, while the EU has

cultivated a complementary role in security and resilience efforts. Today, 23 out of 27 EU member states are also NATO members, reinforcing the deeply interwoven nature of their security strategies. Given that NATO and the EU collectively represent over one billion people and some of the world's largest economies, their influence on global security policy is considerable, making cybersecurity cooperation a cornerstone of transatlantic stability.[238]

The academic literature on the EU-NATO inter-organisational relations closely followed the empirical developments, starting with the years following the St. Malo Declaration (1998) and the Berlin Plus agreements (2003). Due to the rapidly evolving threat landscape, the strategic partnership between the EU and NATO has gained even greater relevance in recent years. The increasing reliance on digital infrastructure, interconnected supply chains, and networked defence systems has widened the attack surface for malicious actors, including state-sponsored cyber operations.

Russia's war of aggression against Ukraine has further exposed vulnerabilities in critical infrastructure, as cyberattacks increasingly complement physical assaults in hybrid warfare strategies. In response to these challenges, the EU and NATO launched the *Task Force on Resilience of Critical Infrastructure* on March 16, 2023[239]. This initiative marked a significant milestone in cybersecurity cooperation, aiming to strengthen resilience across four essential sectors: energy, transport, digital infrastructure, and space.

The final assessment report of the Task Force, published in early 2024, highlighted the growing risks faced by critical infrastructure. The sabotage of the Nord Stream pipelines demonstrated the vulnerability of energy infrastructure, particularly as energy networks become increasingly politicised and weaponized. Similarly, the transport sector emerged as a high-risk domain, given the military's heavy reliance on civil and commercial transport infrastructure for operational mobility. As transport networks become increasingly digitised, the potential for cyberattacks to disrupt military logistics and supply chains has escalated significantly[240]. The report also underscored the fragility of digital infrastructure, particularly the dependence on undersea cables and 5G networks, which pose significant security risks due to their global supply chain dependencies. Meanwhile, the space domain once considered a purely military concern, has become an integral element of cybersecurity discussions, with adversaries developing

[238]Council of the EU and the European Council (2024). EU-NATO cooperation.
[239] NATO. (2023). NATO and European Union launch task force on resilience of critical infrastructure. North Atlantic Treaty Organization, Official Website.
[240]NATO. (2024). Relations with the European Union. North Atlantic Treaty Organization, Official Website.

counter-space capabilities that threaten satellite communications, navigation systems, and intelligence networks[241]. All of this sheds light on the processes of mutual influence, informal interaction and decision-making, practical coordination, and the development of concrete deliverables and outputs by the two organisations.

Over the past two decades, the EU and NATO have taken structured steps to enhance cybersecurity cooperation, integrating policy coordination, joint exercises, and crisis response mechanisms. A key moment in this partnership came in 2016, when NATO and the EU signed the *Technical Arrangement on Cyber Defence*, facilitating operational-level information sharing between NATO's *Computer Incident Response Capability (NCIRC)* and the EU's *Computer Emergency Response Team (CERT-EU)*[242]. This agreement enabled the two organisations to enhance their joint threat intelligence-sharing, cybersecurity planning, and rapid response coordination.

In July 2016, the EU-NATO cooperation entered a new era with the signing of a joint Declaration in Warsaw, followed in December by the publication of a standard set of 42 proposals for implementation. An additional set of proposals was adopted in 2017, bringing the total number of suggested actions to 74. Since then, the EU and NATO have signed two additional joint declarations (in 2018 and 2023), and every year, they publish an implementation report regarding these proposed actions, spanning seven key policy areas. The Warsaw Declaration can now be regarded as a pivotal milestone in the history of EU-NATO relations, standing alongside the St. Malo Declaration and the Berlin Plus agreements. During these years, the EU-NATO relations were characterised more by *deconfliction* than full-fledged cooperation[243]. More recently, however, institutional actors at the higher level have used informal ways to foster closer cooperation between the EU and NATO and to bypass enduring political tensions.[244]

Further demonstrating their deepening partnership, the EU and NATO held the first *Structured Dialogue on Cyber* on October 4, 2024[245]. This initiative was designed to bolster cooperation, providing a platform for enhanced coordination in detecting, deterring, and defending against

[241] *Ibidem.*

[242]NATO, 2024. *Cyber defence*. [online] Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm.

[243] Smith S. J. , Gebhard C, Graeger N., (2019), EU-NATO Relations, Running on the Fumes of Informed Deconfliction. Routledge.

[244]Anagnostakis, D. (2025). "Taming the Storm" of Hybridity: The EU-NATO Relationship on Countering Hybrid Threats – From Functional Overlap to Functional Cooperation. *Defence Studies*, 1-25.

[245] European External Action Service, (2024). *European Union and NATO hold the first Structured Dialogue on Cyber*. The Diplomatic Service of the European Union.

cyberattacks. This dialogue aims to improve crisis response frameworks by facilitating scenario-based discussions, streamlining incident reporting, and ensuring greater operational coordination between the EU and NATO cybersecurity structures.

A significant institutional development in EU-NATO cybersecurity cooperation was establishing the NATO *Integrated Cyber Defence Centre (NICC)* in 2024. This centre is a central hub for cybersecurity coordination between NATO and its partners, including the EU, focusing on cyber threat intelligence, real-time response mechanisms, and AI-driven cybersecurity solutions. As cyber threats grow more sophisticated, particularly with quantum computing and AI-powered cyber warfare, the NICC plays a crucial role in enhancing the resilience of digital networks and critical infrastructure across NATO and EU member states[246]. Recognising the vulnerability of undersea energy infrastructure, NATO has prioritised protection strategies for offshore wind farms and undersea cables, which are vital to Europe's economic and energy security. Cybersecurity efforts now include surveillance and response mechanisms to hybrid threats, cyber-enabled sabotage, and physical attacks on maritime infrastructure. To reinforce these measures further, the EU has proposed the creation of a dedicated fleet of vessels to conduct emergency repairs on undersea cables, ensuring the resilience of transatlantic communications and data security.

Despite these advancements, several challenges continue to hinder the complete optimisation of EU-NATO cybersecurity cooperation. One of the primary difficulties lies in the divergent institutional mandates of both organisations. While NATO is a defence alliance, the EU's security approach is grounded in civilian crisis management and regulatory oversight[247]. These structural differences can create gaps in operational coordination, particularly when responding to cross-border cyber incidents that do not fall neatly within the mandates of either organisation. The EU and NATO must focus on deepening cyber resilience, enhancing legal frameworks, and improving interoperability in cyber operations. The *Structured Dialogue on Resilience,* established under the Task Force on Critical Infrastructure, is expected to be a key instrument for shaping long-term cybersecurity policies and ensuring that both organisations remain adaptable to evolving threats.[248]

---

[246]NATO. (2024). Allies agree new NATO Integrated Cyber Defence Centre. North Atlantic Treaty Organization Official Website.

[247] Anagnostakis, D. (2025). "Taming the Storm" of Hybridity: The EU-NATO Relationship on Countering Hybrid Threats – From Functional Overlap to Functional Cooperation. *Defence Studies*, 1–25.

[248] *Ibidem.*

The EU-NATO cybersecurity partnership remains vital for ensuring the protection and resilience of critical infrastructures. In this era, the harmonisation of cybersecurity policies, the development of joint defence strategies, and the continuous improvement of cyber threat intelligence-sharing mechanisms will determine the effectiveness of transatlantic security in the digital age. By reinforcing technological cooperation, enhancing deterrence capabilities, and maintaining a forward-looking strategic vision, the EU and NATO can fortify the cyber defence architecture of the Euro-Atlantic region, ensuring long-term stability and security.

2.5. Research Puzzle

The literature on cyber defence has significantly expanded over the past decade, reflecting the growing awareness of cyber threats as a core concern in national and international security agendas. Scholarly contributions have thoroughly examined the cybersecurity strategies of major international organisations, particularly NATO and the European Union, elucidating their doctrinal evolution, institutional frameworks, and strategic priorities. However, there remains a conspicuous gap in the academic discourse regarding the practical integration of these cybersecurity frameworks at the national level, especially in the case of non-member states exposed to systemic and persistent cyber threats. This omission is particularly relevant given the hybrid nature of modern geopolitical conflicts, wherein cyberwarfare plays an increasingly central role in undermining state sovereignty, disabling critical infrastructure, and shaping strategic outcomes.

As a non-member yet highly engaged partner of both NATO and the EU, Ukraine offers an empirically rich and analytically compelling case to investigate this phenomenon. Since 2014, and with renewed urgency following the full-scale Russian invasion in 2022, Ukraine has become a geopolitical frontline and a critical test-bed for cyber conflict. The scale, intensity, and coordination of cyberattacks targeting Ukraine's critical infrastructure, primarily attributed to Russian state-sponsored groups, have made the cyber dimension of the conflict a vital theatre of strategic competition. The integration of cyberwarfare into broader military and political objectives during the ongoing war has revealed how digital operations can precede, complement, or even substitute conventional force.

Since the outbreak of the war in February 2022, cyberattacks have targeted a wide array of sectors, from energy grids and railway systems to government platforms and satellite communications, often coinciding with kinetic military operations or political disruption campaigns. These operations have had both tactical and symbolic effects, aiming not only to degrade Ukraine's capabilities but also to destabilise governance, instil fear among civilians, and undermine international confidence. This context presents a unique opportunity to analyse the operational outcomes of cyber resilience, understood not in the abstract but as an empirical response to a multidimensional, high-threat environment. In this setting, Ukraine has undertaken a substantial programme of cybersecurity reform, which has not been developed in isolation. On the contrary, it has been deeply informed by NATO and EU frameworks, including doctrinal principles, technical standards, strategic partnerships, and capacity-building initiatives.

Yet, despite the proliferation of policy documents, strategic roadmaps, and public commitments to cyber cooperation, what remains insufficiently explored is the extent to which NATO and EU frameworks have been integrated into Ukraine's national cybersecurity posture and, more importantly, whether this integration has yielded tangible improvements in resilience. While support and cooperation are often invoked in policy narratives, integration is a higher threshold, requiring institutional adaptation, operational synchronisation, and sustained capacity-building. Understanding whether such integration has occurred and whether it has contributed to Ukraine's ability to anticipate, withstand, and recover from cyberattacks is the core objective of this research.

This thesis, therefore, seeks to address the *relationship between the integration of NATO and EU cybersecurity frameworks and the operational outcomes of national cyber resilience in a conflict-ridden environment.* This research puzzle is analytically significant for two primary reasons. Firstly, it invites a shift from a conceptual understanding of cyber partnerships to an empirical assessment of their implementation. Secondly, it interrogates the functional impact of such integration, moving beyond rhetorical commitments or high-level declarations to focus on measurable changes in resilience and response capacity. The objective is to determine whether the adoption and incorporation of NATO and EU cybersecurity principles, such as regulatory harmonisation, information sharing, joint training, and institutional capacity-building, have contributed to a demonstrable improvement in Ukraine's ability to defend and recover from cyber incidents launched from Russia and targeting its critical infrastructure.

2.6. Research question

The research question that emerges from this puzzle is formulated as follows:

How did the integration of NATO and EU cybersecurity frameworks impact Ukraine's resilience against Russian cyberattacks on critical infrastructures?

This question is structured to invite a causal and explanatory analysis. Rather than merely cataloguing NATO and EU initiatives or describing Ukraine's cybersecurity landscape, it investigates how international cybersecurity doctrines, practices, and institutional designs are translated into national capability. It is concerned with understanding not only the degree of integration but also its tangible outcomes in the context of real-world cyber incidents. Furthermore, focusing on "integration" instead of "support" is methodologically and analytically deliberate. While "support" implies a one-directional, and often vague, provision of resources or expertise, "integration" connotes a deeper, reciprocal, and systemic alignment, wherein NATO and EU cybersecurity frameworks become embedded within national structures, inform regulatory paradigms, shape incident response protocols, and condition strategic decision-making.

2.6.1. Research Hypotheses

The hypothesis guiding this research is thus articulated in the following terms:

NATO and EU cybersecurity frameworks impacted Ukraine's resilience against cyberattacks on its critical infrastructure.

Notably, this hypothesis is not posited in a confirmatory manner. Instead, it is presented as an open proposition, subject to empirical validation through the Ukraine case study. The thesis seeks to assess whether a causal relationship can be identified and, if so, whether the effect has been positive, negligible, or potentially even counterproductive under certain conditions.
This framework defines *the independent variable* as the degree of integration of NATO and EU cybersecurity frameworks into Ukraine's national cybersecurity strategy. This includes legal

harmonisation with the EU's Network and Information Security (NIS) Directives, institutional engagement with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), participation in cyber exercises such as Cyber Coalition, and the operationalisation of joint incident response mechanisms.

The *dependent variables* are twofold. The first pertains to Ukraine's ability to prevent cyberattacks, encompassing anticipatory capabilities, vulnerability management, and deterrence posture. The second involves the speed and effectiveness of Ukraine's responses once cyberattacks occur, including real-time incident management, inter-agency coordination, recovery processes, and the restoration of affected services. These variables are operationalised through the analysis of specific cyber incidents, the examination of institutional developments, and the evaluation of strategic documentation.

2.6.2. Research Method

This thesis employs a qualitative empirical case study approach with Ukraine as the single case. Ukraine is selected not only for its salience as a current target of cyberwarfare but also for the strategic depth of its partnerships with NATO and the EU. The methodological framework is rooted in process tracing, allowing for a longitudinal reconstruction of Ukraine's cybersecurity trajectory in relation to the integration of NATO and EU frameworks.

The case study methodology enables a detailed examination of structural and event-based data. The structural component entails an analysis of Ukraine's cybersecurity policies, legal reforms, and institutional alignments with NATO and EU standards. This includes examining national cybersecurity strategies, cyber incident response frameworks, and sectoral regulatory provisions, especially in critical infrastructure sectors such as energy, finance, and transportation.

The event-based component focuses on cyberattacks with strategic implications for Ukraine's critical infrastructure. Particular attention will be given to the 2015 and 2016 attacks on the Ukrainian power grid, the 2017 NotPetya incident, and a series of cyber operations associated with the 2022 Russian invasion. Each case will be analysed to trace patterns of response, identify institutional performance, and assess the role played by prior integration with NATO and EU frameworks in shaping outcomes.

The empirical analysis will draw on a variety of primary and secondary sources. These include official documents from Ukrainian government agencies, NATO, and the EU; cybersecurity

threat intelligence reports from leading firms such as Mandiant, CrowdStrike, and Microsoft; and quantitative indexes such as the National Cyber Power Index and the Cybersecurity Exposure Index. In addition to these, the analysis will incorporate findings from recent and authoritative reports such as the November 2023 Cyberdefense Report by the Center for Security Studies at ETH Zürich, which critically assesses the implementation of EU Cyber Rapid Response Teams (CRRTs) and NATO's Rapid Reaction Teams, highlighting their limitations and contributions in support of partner states like Ukraine. The report's case study on Ukraine (2022) offers key insights into the formal structures and operational challenges of rapid cyber response internationally.

Moreover, this research integrates up-to-date materials from institutional sources, such as Ukraine's recent agreement to join the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the ENISA-led initiatives to enhance EU-Ukraine cybersecurity cooperation, and the 2023 EU-NATO Joint Final Assessment Report on digital threats and collective resilience. Press releases from the European Council regarding sanctions in response to Russian hybrid threats further enrich the geopolitical context, while analyses by the BBC and other journalistic sources provide valuable data on the public communication and perception of cyber incidents. These sources enhance the empirical robustness of the analysis and allow for triangulation across technical, institutional, and strategic dimensions.

2.6.3. Scope

The third and final chapter of this thesis undertakes a structured empirical analysis to evaluate the relationship between the integration of NATO and EU cybersecurity frameworks and Ukraine's resilience to cyberattacks on critical infrastructure, particularly in the context of Russian hybrid warfare. The analysis adopts both a chronological and thematic approach to trace the evolution of Ukraine's cybersecurity posture and assess the operational consequences of framework integration under conditions of sustained cyber conflict.

The first section of the chapter (3.1) reconstructs the evolution of Ukraine's cybersecurity landscape from the period preceding the 2022 full-scale invasion. It outlines the legal, institutional, and operational components of Ukraine's cyber defence architecture, beginning with the post-2014 reforms that followed Russia's annexation of Crimea. This section highlights Ukraine's early vulnerabilities in the protection of critical infrastructure and examines the initial

steps toward alignment with NATO and EU cybersecurity standards. Particular attention is paid to Ukraine's involvement in initiatives such as NATO's Trust Fund for Cyber Defence and the EU's Cyber East programme, which laid the groundwork for later, deeper cooperation. The section then moves to analyse the escalation of cyber operations during the 2022 war and Ukraine's accelerated integration into Western cyber frameworks, including its participation in the Cooperative Cyber Defence Centre of Excellence (CCDCOE), activation of Cyber Rapid Response Teams (CRRTs), and expanded engagement in multilateral cyber exercises and intelligence-sharing arrangements.

The second section (3.2) presents a series of case studies of Russian cyberattacks targeting Ukraine's critical infrastructures across two key phases: the pre-2022 period of limited cooperation, and the post-invasion period of intensified integration. These include the 2015 and 2016 power grid attacks, and more recent attacks on energy networks, during the 2022–2023 winter. Each case study reconstructs the nature and strategic function of the attack, evaluates its immediate and long-term impact, and assesses the effectiveness of Ukraine's technical and institutional response. Where possible, the analysis identifies whether and how NATO/EU cooperation contributed to improved coordination, response time, damage containment, or recovery efforts.

The final section (3.3) offers a comparative evaluation of Ukraine's cyber resilience across the selected case studies. It synthesises the findings to identify patterns in institutional adaptation, operational effectiveness, and the capacity to withstand or recover from cyberattacks. This section pays particular attention to sectoral vulnerabilities, focusing on energy, and assesses how integration into NATO and EU cybersecurity frameworks may have enhanced Ukraine's ability to prevent, detect, and respond to cyber threats. The analysis also considers persistent gaps and structural challenges that remain despite increased cooperation.

Together, these three sections provide the empirical basis for answering the central research question. By comparing Ukraine's cybersecurity posture before and after its intensified engagement with NATO and the EU, the chapter evaluates the extent to which framework integration has tangibly improved cyber resilience. In doing so, it also reflects on the broader implications for multilateral cybersecurity governance and the potential replicability of this model in other states facing hybrid threats.

CHAPTER III

Cyber Resilience in Wartime: A Case Study on the Impact of NATO and EU Cybersecurity Integration on Ukraine's Defence Against Russian Cyberattacks (2014–2024)

3. Introduction: Objectives and Analytical Strategy

The intensification of cyber warfare in Ukraine since Russia's 2014 annexation of Crimea, and especially since the 2022 invasion, has positioned the country as a prime testing ground to evaluate the effectiveness of international collaboration on cybersecurity matters within the framework of hybrid conflicts. While the previous chapters outlined the strategic and institutional cyber architecture of NATO and EU governance, this chapter focuses on an empirical approach. It seeks to investigate whether the integration in Ukraine of the Euro-Atlantic frameworks has impacted cyber resilience, particularly to the protection of critical infrastructure.

Rather than examining formal structures in isolation, this chapter evaluates their effectiveness in operation by examining Ukraine's cybersecurity evolution and response to specific cyber events. By doing this, it draws on instances of Russian cyberattacks to examine whether more cooperation, via collaborative training, intelligence sharing, technical assistance, and rapid reaction mechanisms, brought measurable gains to Ukraine's prevention, containment, and recovery from cyberattacks.

This qualitative analysis also provides a broad framework for analysing how multilateral cybersecurity frameworks perform under pressure, particularly in wartime, when cyberattacks test political commitments. Furthermore, the experience in Ukraine can teach scholars about the possibilities and limitations of international cybersecurity convergence in conflict zones.

3.1. Ukraine's Cybersecurity Landscape

The evolution of Ukraine's cybersecurity landscape provides a case study of how a state under sustained hybrid aggression can restructure its institutional, legal, and strategic posture in

response to cyber threats. What began as a relatively weak and fragmented digital defence apparatus has become one of the most stress-tested cyber ecosystems in the world. This transformation has occurred not only because of the internal imperative to shield critical infrastructure and preserve sovereignty, but also due to the strategic alignment with NATO and EU frameworks[249]. Frameworks that have functioned both as sources of technical support and as pathways to geopolitical integration. On the legal front, Ukraine has worked to build a dual framework that combines domestic legislation with international obligations. Instruments such as the Budapest Convention on Cybercrime and the EU's Network and Information Security (NIS) Directive have served as starting points for policy development[250]. Simultaneously, the Ukrainian government has adopted national legislation to address the growing frequency and severity of cyberattacks, including cyberterrorist incidents. This legal adaptation not only reflects Ukraine's commitment to protecting its digital sovereignty but also supports its broader political objective of demonstrating readiness for EU accession. With time, cybersecurity, in the Ukrainian context, transformed from a peripheral policy area to a central pillar of national security.[251]

The information sphere has a direct impact on Ukraine's political, economic, and defence systems, forming the basis of post-industrial development. The establishment of a secure cyber environment, where information flows freely but safely, is thought to require a stable, open, and effectively governed information space.[252] Control over the cybernetic domain is equivalent to control over national resilience itself, as demonstrated by the Russian Federation's hybrid war strategy, which operates concurrently in physical, digital, and psychological spaces. In this sense, cyberwarfare is an extension of information warfare rather than a distinct front, and it has a direct impact on the legitimacy of state institutions as well as the operation of vital infrastructure[253].

When the first significant cyberattacks targeted Ukrainian governmental and private systems during the Euromaidan protests in 2013, the urgency of cyber defence became apparent. With the annexation of Crimea and the start of hostilities in the Donbas region in 2014, these incidents marked the beginning of a protracted campaign of cyber aggression that would intensify[254].

[249] CYBER DIIA. (2024). A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience A comprehensive review.
[250] Zinchenko, O. I. (2024). Cyber terrorism: History of Ukraine and current trends. Actual Issues of Modern Science. European Scientific e-Journal, 33, 70-79. Ostrava: Tuculart Edition, European Institute for Innovation Development.
[251] *Ibidem.*
[252] Sopilko, I. (2024). Strengthening cybersecurity in Ukraine: Legal frameworks and technical strategies for ensuring cyberspace integrity. Legal Horizons, 21(2), 69-80.
[253] Bronk C. Collins G. Wallach D. S. (2023). The Ukrainian Information and Cyber War. THE CYBER DEFENSE REVIEW
[254]CYBER DIIA. (2024). A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience A comprehensive review.

Before the kinetic conflict, the cyber component of Russia's hybrid warfare had already developed, paving the way for increasingly complex and well-coordinated cyberattacks against Ukrainian institutions. These attacks were deeply ingrained in psychological and information warfare, in addition to targeting infrastructure and information systems. They revealed the multidimensional nature of cyber conflict, where multiple fronts converge, such as the military, technical, legal, and communicative ones[255]. This has shown the inadequacy of Ukraine's institutional and technical readiness at the time. Initial attacks on governmental websites and media outlets evolved into more complex campaigns, such as the 2015 and 2016 power grid attacks, which demonstrated Russia's ability to cause physical disruption through cyberspace[256].

Ukraine began creating a national cybersecurity architecture from scratch in response to growing cyber threats, particularly following the events of 2014. The state initiated an institutional and legislative development process between 2015 and 2021 with the objective of enhancing cyber governance and operational capability[257]. Although progress was uneven, these efforts set the groundwork for a more organised response to cyber incidents. Fragmentation, ambiguous directives, and inadequate coordination systems continue to hinder proactive threat management and strategic depth.

At the same time, broader geopolitical forces influenced this internal development. Ukraine's foreign and security strategy underwent a significant shift to the west as a result of Russia's aggression, and cybersecurity became a key area of collaboration with NATO and the European Union. Despite the relatively low level of initial engagement with Western partners, such as the EU's Cyber East and EU4Digital programmes and NATO's Cyber Defence Trust Fund, these collaborations offered training and technical assistance[258]. More significantly, they signalled the start of Ukraine's alignment with Euro-Atlantic cybersecurity frameworks, especially in areas such as incident response, cyber hygiene, and critical infrastructure protection. In the sections that follow, the details of these institutional and global developments will be looked at.

The outbreak of the war in February 2022 fundamentally disrupted the operational environment. Russia launched a series of destructive cyberattacks, ranging from data-wiping malware to large-scale Distributed Denial of Service (DDoS) campaigns and satellite jamming, aimed at

[255] *Ibidem.*

[256] Renz, B. (2019). Russian 'Hybrid Warfare': Resurgence and Politicisation. *The RUSI Journal*, *164*(3), 70–71.

[257] Sopilko, I. (2024). Strengthening cybersecurity in Ukraine: Legal frameworks and technical strategies for ensuring cyberspace integrity. Legal Horizons, 21(2), 69-80.

[258] Shelest H. - Omelianenko V. (2023). Policy Paper. EU, NATO and Ukraine. Dream Team or a Triangle. Ukrainian Prism.

damaging Ukraine's command-and-control systems, degrading public services, and instilling fear. These operations were often coordinated with physical military offensives, most notably the cyberattack on February 24, 2022, on the Viasat KA-SAT satellite network, which preceded the invasion by hours and impacted connectivity across Europe[259]. The digital battlefield thus became an extension of kinetic warfare, embedded in Russia's broader strategy of hybrid destabilisation.

As a result of persistent hybrid threats, Ukraine's cybersecurity landscape has undergone significant changes. The nation transitioned from reactive crisis management to a more structured, albeit still unsatisfactory, cyber governance model, despite the institutional and legal frameworks remaining unstable. Notably, Ukraine started to move toward deeper cybersecurity cooperation with NATO and the EU in the post-2014 era. It is unclear, nevertheless, how much this changing architecture improved Ukraine's cyber resilience.

3.1.1. Analysis of Ukraine's cybersecurity architecture and policy before 2022

Building on the broad framework previously described, I now focus on Ukraine's architecture and policies before 2022. This period includes the years following Ukraine's independence to the night before the full-scale invasion in February 2022. I will examine the institutional, strategic, and legislative frameworks Ukraine has implemented in response to growing cyber threats. This section evaluates the coherence, depth, and efficacy of Ukraine's pre-2022 cybersecurity architecture, with a particular focus on its institutional design, legal foundations, and implementation gaps. It does not, however, examine individual cyberattacks, which will be addressed in a subsequent section.

After gaining its independence, Ukraine faced the challenging task of updating its governance and national security structures to meet the new demands of the digital age. It inherited, like many post-Soviet states, a limited cybersecurity culture, a weak digital infrastructure, and little to no prior legal or strategic doctrine for the cyber domain[260]. Historically, institutional capacity in cybersecurity has been lacking. Early progress was further hampered by Ukraine's inherited administrative culture from the Soviet era. Without specific governance, cybersecurity functions were frequently subordinated to more general IT duties, and bureaucratic compartmentalisation

[259] Kvartsiana, K. and Fellowship, R. (2023). *Report Ukraine's Cyber Defense Lessons in Resilience*. [online]
[260] Brantly, A. (2022). Battling the bear. *Cyber Security Politics*, [online] pp.157–171.

hindered strategic coordination. The structures that were in place were disjointed, functionally distinct, and had ambiguous missions. There was a lack of technical expertise within government agencies, and at best, interagency cooperation was informal[261].

Some foundational steps were nonetheless taken during this early period. In 2007, Ukraine established the State Special Communications and Information Protection Service (SSSCIP), intended to serve as the central body for protecting state information resources[262]. In 2009, it also established the Computer Emergency Response Team of Ukraine (CERT-UA), which would later become internationally recognised, including membership in FIRST (Forum of Incident Response and Security Teams)[263]. However, despite these developments, their mandates remained narrow. CERT-UA, for example, lacked the legal authority to issue binding instructions to government or private actors, and its access to real-time threat intelligence was minimal. The agencies often operated in silos, with limited access to shared platforms or interoperable systems. Moreover, they were critically underfunded and lacked the human capital to engage with the fast-evolving landscape of cyber threats[264].

By 2013, it was abundantly evident that Ukraine's cybersecurity capacity fell short of the demands it would soon face. The nation had not yet developed a comprehensive national cybersecurity policy or committed itself to aligning policies and laws with those of European or NATO models. There was also no functional classification system for critical infrastructure, and no mandatory reporting framework for cyber incidents. Furthermore, government networks were frequently outdated, leaving them vulnerable to exploitation[265].

The events of 2013–2014, specifically the Euromaidan protests, the subsequent Russian annexation of Crimea, and the outbreak of conflict in Eastern Ukraine, marked a decisive inflexion point. These geopolitical shocks were accompanied by an escalation of cyber aggression, including the defacement of government websites, data exfiltration from ministries, and disruptions to infrastructures. They exposed, in real time, the profound vulnerability of Ukraine’s information systems and the absence of a coordinated national response mechanism.

---

[261] *Ibidem.*

[262] State Sites of Ukraine (2025). *The history of State Cyber Protection Center*. [online] Scpc.gov.ua. Available at: https://scpc.gov.ua/en/history.

[263] News, T.H. (2025). *CERT-UA Reports Cyberattacks Targeting Ukrainian State Systems with WRECKSTEEL Malware*. [online] The Hacker News.

[264] *Ibidem.*

[265] Sopilko, I. (2024). Strengthening cybersecurity in Ukraine: Legal frameworks and technical strategies for ensuring cyberspace integrity. Legal Horizons, 21(2), 69-80.

More importantly, they signalled the formal beginning of what would become a persistent and escalating campaign of hybrid warfare by the Russian Federation[266].

Ukraine started a deliberate restructuring of its cyber governance system in response to this new threat environment. This change was both strategic and reactive; it sought to modernise the legal system in line with international standards progressively, signal political alignment with Western partners, and build institutional resilience. The Ukrainian state started a comprehensive campaign to define, codify, and institutionalise cybersecurity as a matter of national defence between 2014 and 2022[267].

A significant legislative milestone in this regard was the Law on the Basic Principles of Cybersecurity, adopted in 2017[268]. This law was the first to establish a comprehensive governance framework for cybersecurity in Ukraine. Notably, the law introduced the concept of a national cybersecurity system (NCS) comprising multiple actors, however, it failed to establish unified operational protocols, common terminology, or procedural standards across these actors. Nonetheless, it formally defined the responsibilities of various state bodies and established a division of labour across sectors[269]. The SSSCIP was affirmed as the national policy coordinator, with tasks ranging from strategic oversight and regulatory development to the protection of state information systems and critical infrastructure[270]. CERT-UA was tasked with continuous monitoring, incident coordination, and information sharing in response to threats. The Security Service of Ukraine (SBU) was granted authority over counterintelligence and the prevention of cyberespionage, while the Cyber Police, under the Ministry of Internal Affairs, was assigned the task of investigating cybercrime. The Ministry of Defence and the General Staff of the Armed Forces were responsible for military cyber operations, while sectoral regulators such as the National Bank of Ukraine were entrusted with protecting specific domains, including financial infrastructure[271].

---

[266] Zinchenko, O. I. (2024). Cyber terrorism: History of Ukraine and current trends. Actual Issues of Modern Science. European Scientific e-Journal, 33, 70-79. Ostrava: Tuculart Edition, European Institute for Innovation Development.

[267] CYBER DIIA. (2024). A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience A comprehensive review.

[268] Svintsytskyi, A.V. (2022). The system of cybersecurity bodies in Ukraine. Revista Científica General José María Córdova, 20 (38), 287-305.

[269] *Ibidem.*

[270] scpc.gov.ua. (2024). *The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine (SCPC SSSCIP) is increasing technical capabilities of the National Center for Reserving State Information Resources.* [online]

[271] Svintsytskyi, A.V. (2022). The system of cybersecurity bodies in Ukraine. Revista Científica General José María Córdova, 20 (38), 287-305.

On paper, this architecture marked a significant step towards a multi-layered and mature cybersecurity ecosystem. Still, the practical value of this approach was far more limited. Particularly between the SBU and the Cyber Police in cybercrime investigations and between SSSCIP and CERT-UA in information protection and response coordination, there were notable overlaps despite the law's ambition to assign clear roles and responsibilities[272]. Moreover, the legislation failed to establish legally enforceable rules for inter-agency cooperation or safe channels for intelligence flow. The resulting gaps caused delays in threat mitigation, inefficiencies, and duplication. In crises, where real-time information flow and coordinated action are vital, this lack of coordination systems proved especially troublesome. Agencies claimed different incident classification systems and no common situational awareness tool[273].

Crucially, the law also lacked technical and legal precision. It did not define essential concepts such as "cyberattack," "cyber incident," or "cyberterrorism," terms that would become increasingly relevant as the intensity of cyber conflict escalated. This semantic vagueness created complications for prosecution and hindered Ukraine's ability to respond effectively to incidents in legal terms[274]. Moreover, the law did not provide a framework for public-private collaboration in cyber incident handling, even though most critical infrastructure in Ukraine, especially in sectors such as energy, transportation, and telecommunications, is operated by private actors[275].

One of the most persistent obstacles to Ukraine's cyber resilience before 2022 was the mismatch between its criminal justice framework and the complexity of modern cyber threats. The Ukrainian Criminal Code[276], as of 2020, included only a few provisions relevant to cybercrime, most notably Articles 361, 361-1, and 362, which addressed unauthorised interference in information systems, unlawful access, and data destruction. However, these provisions were outdated, limited in scope, and failed to account for the diverse range of contemporary threats such as ransomware, DDoS attacks, phishing campaigns, and state-sponsored cyberespionage[277].

---

[272] Kvartsiana, K. and Fellowship, R. (2023). *Report Ukraine's Cyber Defense Lessons in Resilience*. [online]
[273] *Ibidem.*
[274] Svintsytskyi, A.V. (2022). The system of cybersecurity bodies in Ukraine. Revista Científica General José María Córdova, 20 (38), 287-305.
[275] Axon, L., Saunders, J., Esteve-González, P., Carver, J., Dutton, W., Goldsmith, M., & Creese, S. (2025). Private-public initiatives for cybersecurity: the case of Ukraine. *Journal of Cyber Policy*, 1–24.
[276] Criminal Code of Ukraine, Arts. 361–362, No. 2341-III of 5 April 2001, as amended, available at: https://www.wipo.int/wipolex/en/text/438599
[277] Svintsytskyi, A.V. (2022). The system of cybersecurity bodies in Ukraine. Revista Científica General José María Córdova, 20 (38), 287-305.

The legislation also lacked a gradation of offences or differentiation between civilian, critical, and military targets. Penalties were often vague, unenforceable, or disproportionate, making prosecution challenging.

Deficits in procedural law exacerbated these substantive legal inadequacies. Because the Code of Criminal Procedure lacked procedures for gathering, preserving, and admitting digital evidence, prosecutors found it challenging to put together legally strong cases. Law enforcement and judicial agencies had limited access to forensic techniques, which were scarce, sometimes understaffed, lacked defined evidential standards, and were only available in a few locations. Legal responsibility was further weakened by the courts' inability to evaluate the technological dependability of digital assets[278].

Adding to the problem was the inconsistent application and enforcement of cybercrime provisions across jurisdictions. Law enforcement agencies often differed in how they classified or pursued cyber offences, leading to systemic underreporting, uneven investigative practices, and unreliable national statistics[279]. While the Cyber Police recorded tens of thousands of incidents annually, successful prosecutions remained low, and conviction data was frequently opaque or unpublished, undermining public trust in the state's ability to deliver justice in the cyber domain[280]. Ukraine's legal framework also struggled to integrate its international obligations, especially those under the Budapest Convention on Cybercrime, which was signed in 2006. While the Convention provides a detailed framework for cross-border cooperation, expedited data preservation, and mutual legal assistance, Ukraine had yet to fully transpose many of its provisions into domestic law by 2022[281]. Notably, the country lacked a centralised 24/7 contact point for international cybercrime coordination and had not adopted rules requiring Internet Service Providers (ISP) or digital platforms to retain metadata or subscriber information. These gaps critically impaired Ukraine's capacity to participate in transnational investigations, especially those involving rapid data exchange and procedural interoperability with institutions such as Europol, Eurojust, or Joint Investigation Teams (JITs)[282].

---

[278] *Ibidem.*

[279] Antoniuk, D. (2025). *Ukrainian cyber market grows amid war but still lacks support and funding, report says*. [online] Therecord.media.

[280] *Ibidem.*

[281] Council of Europe (2024). *CyberEast+ Activities*. [online] Cybercrime.

[282] Svintsytskyi, A.V. (2022). The system of cybersecurity bodies in Ukraine. Revista Científica General José María Córdova, 20 (38), 287-305.

Ukraine's poor control of cybercrime has impeded further cooperation with Euro-Atlantic institutions[283]. It is necessary to close these legal and procedural gaps for Ukraine's full participation in EU and NATO cybersecurity cooperation frameworks, as well as to enhance national cyber resilience and expedite Ukraine's integration into the European Digital Single Market. A key prerequisite for Ukraine's integration into the larger European security framework is legal congruence in the areas of data protection, digital sovereignty, and evidential harmonisation[284].

In recognition of the limitations of its legal framework, Ukraine sought to complement its cybersecurity efforts with strategic policy documents that articulate a coherent national vision. Presidential Decree No. 96/2016, which established the 2016 Cybersecurity Strategy, was a significant turning point in this area[285]. It outlined several strategic goals, including safeguarding vital infrastructure, advancing state cyber capabilities, enhancing interagency collaboration, and strengthening foreign alliances, particularly with the European Union and NATO. It also demanded the establishment of a single threat monitoring system, the standardisation of response procedures across industries, and the development of cyber units within the Armed Forces[286].

Significantly, the Strategy recognised "Cyberspace" as a separate domain of hostilities, alongside the traditional realms of Earth, Air, Sea, and Space, reflecting international trends in military doctrine. It explicitly described the National Cybersecurity System and delineated the responsibilities of key actors, offering, for the first time, a systemic framework for cyber governance[287].

Strategic coordination was assigned to the National Coordination Centre for Cybersecurity (NCCC), an inter-agency body operating under the National Security and Defence Council of Ukraine. The NCCC was tasked with monitoring threat trends, coordinating national response efforts, and overseeing the implementation of cybersecurity objectives across ministries and government institutions. However, the NCCC lacked permanent staff and operational autonomy. It functioned more as a secretariat of the National Security and Defence Council rather than a full-fledged inter-agency command body[288].

---

[283]Digital Watch Observatory. (2024). *Cybersecurity Strategy of Ukraine | Digital Watch Observatory*. [online]
[284]FREE NETWORK. (2021). *Ukraine's Integration into the EU's Digital Single Market*. [online]
[285]Svintsytskyi, A.V. (2022). The system of cybersecurity bodies in Ukraine. Revista Científica General José María Córdova, 20 (38), 287-305.
[286] *Ibidem.*
[287] *Ibidem.*
[288] *Ibidem.*

Although the Strategy provided a clear intellectual framework, it was challenging to implement in practice. The strategy was operationalised through the introduction of Annual Action Plans. However, they failed due to a lack of political will, poor inter-ministerial cooperation, and insufficient funding. Because of ingrained institutional inertia or a lack of technical capability, ministries frequently failed to carry out their designated responsibilities.[289] At the same time, it was challenging to track progress and impose accountability in Ukraine due to a lack of reliable performance indicators and inadequate reporting systems. Furthermore, Ukraine was unable to anticipate capacity shortfalls because it did not regularly conduct national cybersecurity preparedness exercises or cybersecurity maturity assessments. Despite international support and donor-funded initiatives, many of the Strategy's original objectives remained only partially achieved by the end of its policy cycle.[290]

The militarised and state-centric focus of the 2016 framework was another significant drawback, which led to a lack of participation from non-governmental groups. Although public-private partnerships (PPPs) were promoted in theory, their implementation was hindered by a lack of institutional trust, incentives, and clear regulations. Similarly, despite being some of the most creative and agile players in Ukraine's broader cyber ecosystem, the academic community and civil society organisations were mainly excluded from the process of developing policies and coordinating operations[291]. However, unofficial partnerships developed. NGOs and private players frequently filled operational and policy gaps by providing incident detection, training assistance, and threat intelligence analysis. Hardly were these contributions codified in official policy texts. Local governments and critical service providers, including those in the energy, transportation, and telecommunications sectors, operated without comprehensive guidance on how to comply with national cybersecurity standards or participate in national-level crisis response planning[292].

In light of these weaknesses, a revised Cybersecurity Strategy was adopted in 2021 through Presidential Decree No. 447/2021[293]. This updated strategy led towards a more holistic and forward-looking vision for national cyber defence. It emphasised interoperability between

[289]Kvartsiana, K. and Fellowship, R. (2023). *Report Ukraine's Cyber Defense Lessons in Resilience*. [online]
[290] National Security and Defense Council of Ukraine. (2023). *National Security and Defense Council of Ukraine*. [online]
[291]Kvartsiana, K. and Fellowship, R. (2023). *Report Ukraine's Cyber Defense Lessons in Resilience*. [online]
[292]DAI Global, LLC (2021). *USAID CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE REVIEW OF THE REGULATORY FRAMEWORK FOR CRITICAL INFRASTRUCTURE CYBERSECURITY IN UKRAINE: LEGISLATIVE ASSESSMENT REPORT*.
[293] National Security and Defense Council of Ukraine (2021). *The President of Ukraine approved a new Cybersecurity Strategy of Ukraine*. [online] National Security and Defense Council of Ukraine.

Ukraine's cybersecurity architecture and those of NATO and the EU, and explicitly integrated cyber defence into military doctrine. Acknowledging the importance of societal resilience, the strategy also proposed increased investment in research and development, cyber education, and public awareness initiatives[294].

The establishment of specialised military cyber units, increased financing for cybersecurity research, and the formalisation of collaboration between government, academia, and civil society were among the main objectives. In line with its broader objective of integrating into the EU's digital governance framework, the plan highlighted Ukraine's commitment to align with European cybersecurity standards, particularly those outlined in the EU's NIS Directive.

Despite this ambitious agenda, early assessments of implementation revealed familiar obstacles. Institutions struggled with technical capacity, governance, budgetary limitations, outdated curricula, insufficient funding, and underrepresentation of civil society organisations in decision-making structures, despite their proven capacity.

Thus, while the 2021 Strategy introduced more inclusive and forward-leaning objectives, many of the structural barriers that hindered earlier efforts persisted. Although Ukraine made significant strides toward a more responsive and cohesive cybersecurity strategy, its overall resilience in the years leading up to 2022 was still hampered by deficiencies in institutional capacity, legal enforcement, and implementation. Ukraine tested regional versions of the Center in Dnipro and Odesa, areas with heightened vulnerability to geopolitical risk, to increase geographic coverage. Coordination between CERTs, regional administrations, and central agencies was unequal by 2021, and regional integration into the national cyber response structure was still lacking.

While state-led reforms progressed slowly, civil society groups and volunteer-based cybersecurity communities emerged as some of Ukraine's most dynamic contributors to cyber defence. Organisations like the Ukrainian Cyber Alliance (UCA), RUH8, and others played key roles in uncovering malware campaigns (e.g., Snake and X-Agent), tracking espionage efforts, and even mounting counter-offensives in cyberspace. These actors performed functions that often exceeded the capacity of state agencies[295].

---

[294] *Ibidem.*

[295] Miller, C. (2016). *Inside The Ukrainian 'Hacktivist' Network Cyberbattling The Kremlin*. [online] RadioFreeEurope/RadioLiberty.

The panorama of cyber risks was brought to light throughout the 2013–2021 timeframe. It emphasised the necessity of a proactive strategy for cybersecurity, giving government and IT protection top priority due to their importance to both national security and the smooth operation of society. Ukraine made significant efforts to create a more robust and well-coordinated cybersecurity infrastructure. A thriving civil society, which made significant contributions to operational capability and technical innovation, was also involved in these initiatives, alongside state institutions. Disjointed institutional duties, imprecise legislative definitions, and a lack of financing and technological know-how, however, continued to impede the national framework.
The adoption of strategic documents, legislative changes, and increased interaction with foreign partners enabled Ukraine to make significant progress despite these challenges. Even though it was still being developed, the general structure signalled a change in direction towards increased readiness. These fundamental steps served as the cornerstone for the more resilient and flexible cybersecurity posture that developed in response to the full-scale Russian invasion in 2022, even if ongoing coordination and enforcement issues highlighted the system's weaknesses.

3.1.2. Towards Strategic Unity: NATO and EU cooperation after Crimea

Ukraine's national security posture underwent a significant change in 2014 when Russia annexed Crimea. The event was an early example of Russia's developing hybrid warfare tactic and constituted a serious violation of Ukraine's territorial integrity. To destabilise and conquer the Ukrainian land, a concerted combination of misinformation, hacking, irregular military operations, and proxy warfare was employed.
Media supported by the Kremlin attempted to undermine Kyiv's authority and incite separatist sentiment, especially in Crimea and eastern Ukraine[296]. At the same time, cyberattacks that were often ascribed to hacking groups with ties to the Kremlin attacked vital infrastructure and government communications. Additionally, the campaign included unidentified armed individuals known as "Little Green Men," who secretly seized important locations while hiding their country's allegiance. These forces, which subsequently turned out to consist of PMC Wagner operatives, special units, and Russian airborne troops, were prime examples of Russia's

[296] Rinaldi, S. (2024). *10 years of Russian annexation of Crimea, reflections on the role of PMCs in hybrid warfare - ICoCA Blog*. [online] ICoCA Blog.

strategic use of plausible deniability to obscure the distinction between state and non-state actors and postpone an international reaction[297].

This operation's hybrid design highlighted the shortcomings of conventional defensive frameworks and exposed serious flaws in Ukraine's information and cyber systems. Ukraine responded by starting a deliberate transition towards closer ties with the European Union and NATO, especially in the field of cybersecurity. At the same time, the annexation revealed serious weaknesses in the EU and NATO reaction systems, which were ill-equipped to handle threats with hybrid strategies and ambiguity. This dual realisation spurred institutional reforms both within Ukraine and among its Western partners, leading to a closer alignment with NATO and EU cybersecurity norms and practices[298].

In the immediate aftermath, Ukraine significantly deepened its cooperation with NATO[299]. The basis of this effort was the 2014 launch of the NATO Cyber Defence Trust Fund, led by Romania and backed by multiple allies. This initiative supported the development of Incident Management Centres (IMCs), forensic laboratories, and specialised training programs to bolster Ukraine's cyber response capacity. By 2018, with Trust Fund support, Ukraine had established the in Dnipro the Cybersecurity Situation Centre (CSC), designed as a central node for real-time threat detection, coordinated incident response, and intelligence-sharing among state actors[300].

The CSC faced challenges with divided authority, despite promoting the development of secure communication systems, cyber incident databases, and protocol-testing exercises, as well as enhancing interagency collaboration. The overall coherence of Ukraine's cyber defence strategy was limited since it was challenging to bring together agencies that frequently remained to function in silos due to a lack of legal authority to implement instructions.

At the same time, Ukraine became the leading beneficiary of NATO's Science for Peace and Security (SPS) Programme. Between 2014 and 2017, over €10 million was allocated to enhance Ukraine's cyber preparedness, notably through the modernisation of digital command-and-control systems[301]. Cooperation was further institutionalised through Memoranda of Understanding and Ukraine's regular participation in NATO-led cyber defence exercises such

---

[297] *Ibidem.*

[298] Mattis, J. & Hoffman, F.G. (2005) *Future warfare: the rise of hybrid wars.* Annapolis, MD: U.S. Naval Institute. Proceedings 131

[299] NATO (2019). *Relations with Ukraine*. [online] NATO.

[300] Constantin Ionita, C. (2016). *UKRAINE Cyber Defence NATO Trust Fund*. [online]

[301] North Atlantic Treaty Organization.(2015). Fact Sheet, NATO's practical support to Ukraine.

as Cyber Coalition and Locked Shields, which significantly advanced interoperability with allied defence protocols[302].

Another central theme in Ukraine's Annual National Programs (ANPs) with NATO was cybersecurity. These initiatives served as a roadmap for aligning Ukraine's cybersecurity training, education, and regulatory frameworks with NATO requirements. Despite not being a member, Ukraine improved its reputation and established itself as a valuable participant in NATO's cybersecurity ecosystem by consistent participation in joint exercises and doctrinal alignment[303].

Simultaneously, Ukraine launched an ambitious process of integration with the European Union. This was primarily driven by the EU-Ukraine Association Agreement and complemented by initiatives such as EU4Digital and Cybersecurity East, which promoted alignment with the EU's Network and Information Systems (NIS) Directive. Specifically, the EU Cybersecurity East Project (2019–2022) played a critical role in facilitating joint exercises, reinforcing CSIRT (Computer Security Incident Response Team) collaboration, and advancing the institutional adoption of EU cyber norms[304].

At the same time, the EU started incorporating cybersecurity into its larger frameworks for security and foreign policy. The 2015 Council Conclusions on Cyber Diplomacy and the Cyber Diplomacy Toolbox, which established procedures for coordinated diplomatic reactions to cyber crises, were significant advancements. Through channels like TAIEX (Technical Assistance and Information Exchange), Ukraine designated as a strategic partner, received substantial technical help to improve CSIRT performance and bring its laws into compliance with the NIS and NIS2 Directives[305].

Ukraine's gradual integration into the EU Digital Single Market was further exemplified by the mutual recognition of Diia.Signature, its national e-signature system, and agreements on EU-wide roaming. Ukraine also joined the Digital Europe Programme in 2022. Notably, just before the full-scale invasion, Ukraine hosted an EU Cyber Rapid Response Team (CRRT) under the PESCO framework, marking a milestone in operational cyber collaboration between the EU and Ukraine[306].

---

[302] Spînu, N. (2020). *Ukraine Cybersecurity Governance Assessment*. [online]
[303]NATO (2019). *Relations with Ukraine*. [online] NATO.
[304]European Union (n.d.). *EU support for Ukraine | European Union*. [online] european-union.europa.eu.
[305] *Ibidem.*
[306] Grossman, T. (2023). ETH Library Cyber Rapid Response Teams: Structure, Organization, and Use Cases. *Center for Security Studies (CSS), ETH Zürich*. [online]

Notwithstanding these developments, access to specific EU threat intelligence platforms, strategic policy forums, and financial instruments remained restricted due to Ukraine's non-member status. Political unpredictability, resource shortages, and bureaucratic inefficiency were among the domestic barriers that hindered the full implementation of changes supported by external sources.

Over time, Ukraine's bilateral engagements with NATO and the EU began to converge into a de facto trilateral partnership. This evolution was underscored by the EU-NATO Joint Declarations of 2016, 2018, and 2023, which established structured cooperation frameworks addressing cybersecurity, critical infrastructure resilience, and hybrid threat mitigation. These declarations increasingly included provisions for Ukrainian participation, particularly in cyber crisis coordination[307].

On a technical level, the 2016 EU-NATO Technical Arrangement on Cyber Defence enabled the real-time sharing of information and joint incident management between CERT-EU and NATO's NCIRC. Although Ukraine was not a formal signatory, it nonetheless benefited from improved interoperability, reinforcing its integration with Western cybersecurity ecosystems[308].

Ukraine's designation as a NATO Enhanced Opportunities Partner (EOP) further expanded its involvement in cybersecurity policy dialogues, scenario planning, and exercises. This status also empowered Ukraine to advocate more actively for trilateral coordination in domains such as strategic communication, hybrid threat analysis, and coordinated cyber response.

The EU's growing recognition of cybersecurity as a foundation of defence policy accelerated Ukraine's integration. The 2020 EU Cybersecurity Strategy and the 2022 Strategic Compass identified Ukraine as a key partner in shaping collective cyber resilience. The deployment of the EU Cyber Rapid Response Team (CRRT) shortly before the 2022 invasion underscored the operational maturity of this partnership.

By 2022, Ukraine was actively participating in Euro-Atlantic security frameworks, rather than merely receiving cybersecurity assistance. Over 200,000 IT experts work in Ukraine's booming tech industry, which has led to the establishment of both institutional and grassroots programs like the BRAVE1 defence tech cluster and the IT Army of volunteers. Both offensive and

[307] Shelest H. - Omelianenko V. (2023). Policy Paper. EU, NATO and Ukraine. Dream Team or a Triangle. Ukrainian Prism.
[308] *Ibidem.*

defensive cyber capabilities were produced by these initiatives, and they were essential in the early stages of the full-scale invasion[309].

In addition to strengthening its resilience as a country, Ukraine's inventiveness under pressure has an impact on how NATO and the EU see collaboration, deterrence, and cybersecurity policy. Ukraine's transition by 2022 signified a significant change in the field of international cyber cooperation, as it was both a recipient and a co-architect of Euro-Atlantic cyber rules.

3.1.3. The 2022 War and the Strategic Role of Cyberattacks

Years of rising tensions stemming from historical, geopolitical, and security issues culminated in Russia's invasion of Ukraine in February 2022. Russia reacted violently to Ukraine's move towards Euro-Atlantic integration. It carried out actions that demonstrated Moscow's goal of regaining control over its immediate neighbours and thwarting NATO's eastward expansion, which it presented as a direct danger to its strategic objectives. Destabilising Ukraine's democratic government, regaining territorial control, and using force to alter the European security system were the goals of the full-scale military invasion in 2022. However, geographical acquisition by itself no longer determines success or failure in the context of modern warfare.

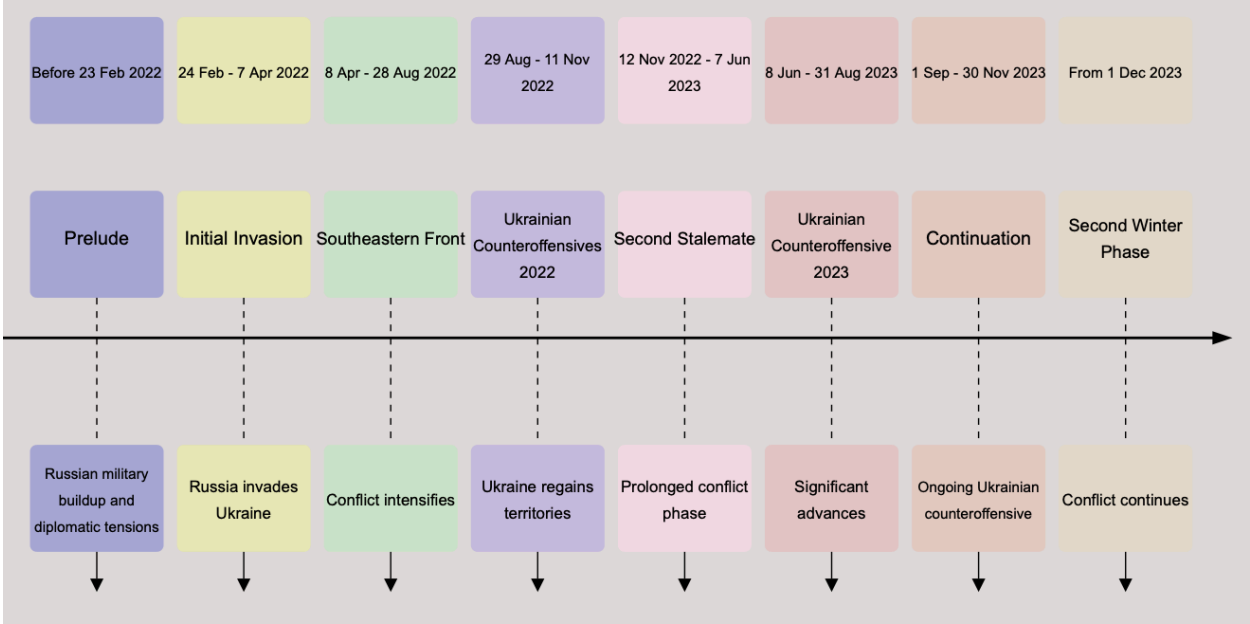
Since digital infrastructure is just as crucial in today's globe as physical territory, cyberspace is an essential theatre of battle. This is particularly true in Ukraine, a nation that has undergone significant digital transformation and whose capacity to maintain information security, operational coordination, and national morale through cyberspace has been crucial to its resilience during the conflict.

However, this military effort did not develop in a straight path. Instead, it developed in several stages, each with changing goals, levels of intensity, and geographic emphasis, patterns that were reflected in the application and modification of cyber operations[310].

[309] *Ibidem.*

[310] Brachiella A. (2022). Policy paper number 281. Cyberattacks In Russia's hybrid war against Ukraine, and its ramifications for Europe. Notre Europe, Jacques Delors Institute.

Figure 7: Phases of Russian Full-Scale Invasion 2022-2023 (recreated)



Source: CYBER DIIA. (2024). A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience. A comprehensive review.

The war shifted from the initial shock phase of February 2022 into a long-term war of attrition, characterised by renewed Russian offensives and Ukrainian counter offensives, as shown in Figure 7. These shifting stages had a significant impact on the cadence and targeting logic of Russia's cyberattacks, which changed tactically and strategically in response to shifting battlefield conditions.

The cyber dimension did not materialise in a series of massive attacks capable of completely paralysing Ukrainian critical infrastructure, as was initially anticipated following the start of the war. Instead, cyber operations were incorporated in ways that were more focused, persistent, and psychologically oriented. For example, destructive malware like HermeticWiper was used by Russia on the eve of the invasion, compromising hundreds of computer systems across various industries, including government, finance, energy, and aviation. Soon after, tens of thousands of modems were rendered inoperable by an AcidRain malware attack against the Viasat satellite communications network[311]. The attack is a perfect example of how cyber operations and kinetic

[311] Schulze M. - Kerttunen M. (2023). Cyber Operations in Russia's War against Ukraine Uses, limitations, and lessons learned so far. Stiftung Wissenschaft und Politik German Institute for International and Security Affairs.

military action are directly synchronised by interfering with Ukraine's military and governmental communications at a critical juncture.

Russia's transition to a fully hybrid warfare model, in which cyberattacks were employed to confuse targets and soften them before or in conjunction with conventional strikes, was reflected in this integration. For instance, Ukraine's leading telecom provider, Ukrtelecom, was the target of a concerted wave of cyberattacks on March 28, 2022, which reduced nationwide connectivity to just 13% of its pre-war level. Concurrently, DDoS attacks disrupted financial and governmental websites, hindering institutional responses during ongoing military escalations[312]. On May 7, Odesa's City Council was the target of a cyberattack just before a missile strike on the city's residential areas. By looking at these events, we can understand the strategic use of cyberattacks but also how Russia weaponized cyberspace to destabilise and disorient both civilian and governmental entities in advance of physical assaults.

Although the early operations were sophisticated and extensive, Russia shifted its approach during the war, transitioning from massive attacks to ongoing, medium- and low-scale cyber harassment. In addition to state institutions, these operations also targeted media outlets, financial institutions, non-governmental organisations, and educational institutions[313]. As demonstrated by intimidation messages inserted into system breaches, news platform vandalism featuring banned Russian symbols, and disinformation campaigns meant to demoralise the populace, psychological warfare was a recurrent goal. One prominent instance was when the Ukraine 24 television channel was hacked to show a deep fake video of President Zelensky's call for surrender[314]. However, the effectiveness of these strategies was undermined by the strong opposition from the Ukrainian people.

Russia gave espionage and data exfiltration more importance as the war progressed. The LoadEdge backdoor malware and the MarsStealer operation are well-known instances that compromised user credentials in the financial, government, and civilian domains[315]. Despite being frequent and extensive, these operations did not provide Russian forces with any apparent advantages. Instead, their main impact was harassment and the build-up of disjointed intelligence.

---

[312]Bagwe, M. (2025). *Ukraine Experiences Internet Outage - and Russia May, Too*. [online] Cio.inc.

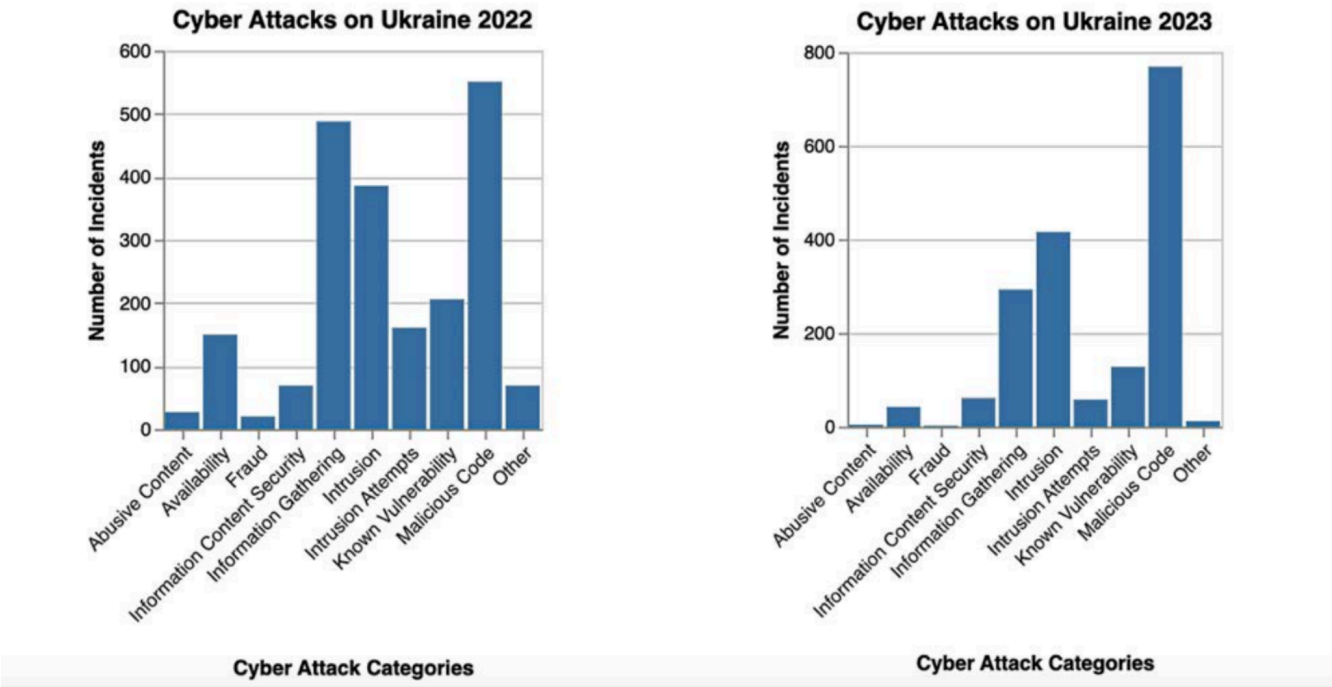
[313] Brachiella A. (2022). Policy paper number 281. Cyberattacks In Russia's hybrid war against Ukraine, and its ramifications for Europe. Notre Europe, Jacques Delors Institute.

[314]Allyn, B. (2022). Deepfake Video of Zelenskyy Could Be 'Tip of the Iceberg' in Info war, Experts Warn. *NPR*. [online] 16 Mar.

[315] Andrii Bezverkhyi (2022). *Detect Mars Stealer Cryptojacking Malware*. [online] SOC Prime.

The type of cyberattacks that were launched in 2022 and 2023 also reflects this shift in strategic focus. To further explain this concept, 11,922 cyber incidents occurred in Ukraine during the war's active phase.[316] As shown in the comparative data below (Figure 8), while 2022 was marked by a high frequency of disruptive malware and information gathering, the 2023 data show a relative rise in intrusion-based activities and exploitation attempts, alongside a notable spike in unclassified or complex attacks under the 'Other' category.

Figure 8: Cyberattacks in 2022-2023



Source: CYBER DIIA. (2024). A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience A comprehensive review.

This shift points to an evolving focus on sustained access, credential harvesting, and system infiltration, hallmarks of long-term surveillance and control rather than one-off disruption. These developments further confirm the integration of cyber operations into Russia's broader military strategy.

[316] CYBER DIIA. (2024). A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience A comprehensive review.

The ability of cyberattacks in 2022 to intensify physical destruction by upsetting the information environment was another factor contributing to their strategic importance. This strategy was prompted by Russia's information-confrontation doctrine, which places more emphasis on psychological and informational disruption than on direct military utility. False reports, including made-up announcements regarding President Zelensky's health, were broadcast on radio stations and news tickers that were taken over[317]. Russia's emphasis on information warfare as a crucial front in the larger conflict was reflected in these actions.

The invasion prompted non-state cyber actors to mobilise in tandem with the state-sponsored operations. An ongoing campaign against Russian infrastructure was initiated by international organisations, such as Anonymous, and pro-Ukrainian collectives, including the IT Army of Ukraine. These entities engaged in DDoS attacks, data leaks, and symbolic hacks, such as breaching Russian state media or leaking personal data of military officials[318]. These efforts significantly disrupted Russian digital assets and damaged the perceived invulnerability of its cyber defences. From Moscow's perspective, such attacks could be interpreted as indirect Western aggression, fuelling the risk of escalation.

Additionally, the war's strategic cyber component had tangible effects beyond Ukraine. Wind turbines in Germany were disabled as a result of the Viasat satellite attack, which also caused long-lasting connectivity problems throughout Europe. Smaller operations, particularly against Eastern European borders and logistics systems, demonstrate the war's wider cyber reach, despite the fact that Russia has not launched many large-scale retaliatory cyberattacks against NATO states[319]. This demonstrates how cyber conflict is becoming increasingly transnational, with linked infrastructures turning localised attacks into regional or even worldwide disruptions.

Until 2025, Russian actors continued to devise new strategies and refine their existing ones. Advanced malware, such as CaddyWiper and AcidPour, which targeted organisations like the Kyivstar mobile operator, was released at the end of 2022 and the beginning of 2023. Improved insider support, coordination, and secrecy were characteristics of these attacks, indicating that Russian cyber capabilities were developing in the context of a protracted conflict[320].

---

[317] Antoniuk, D. (2022). *Hacked Ukrainian radio stations broadcast fakes about Zelensky's health*. [online] The Kyiv Independent.

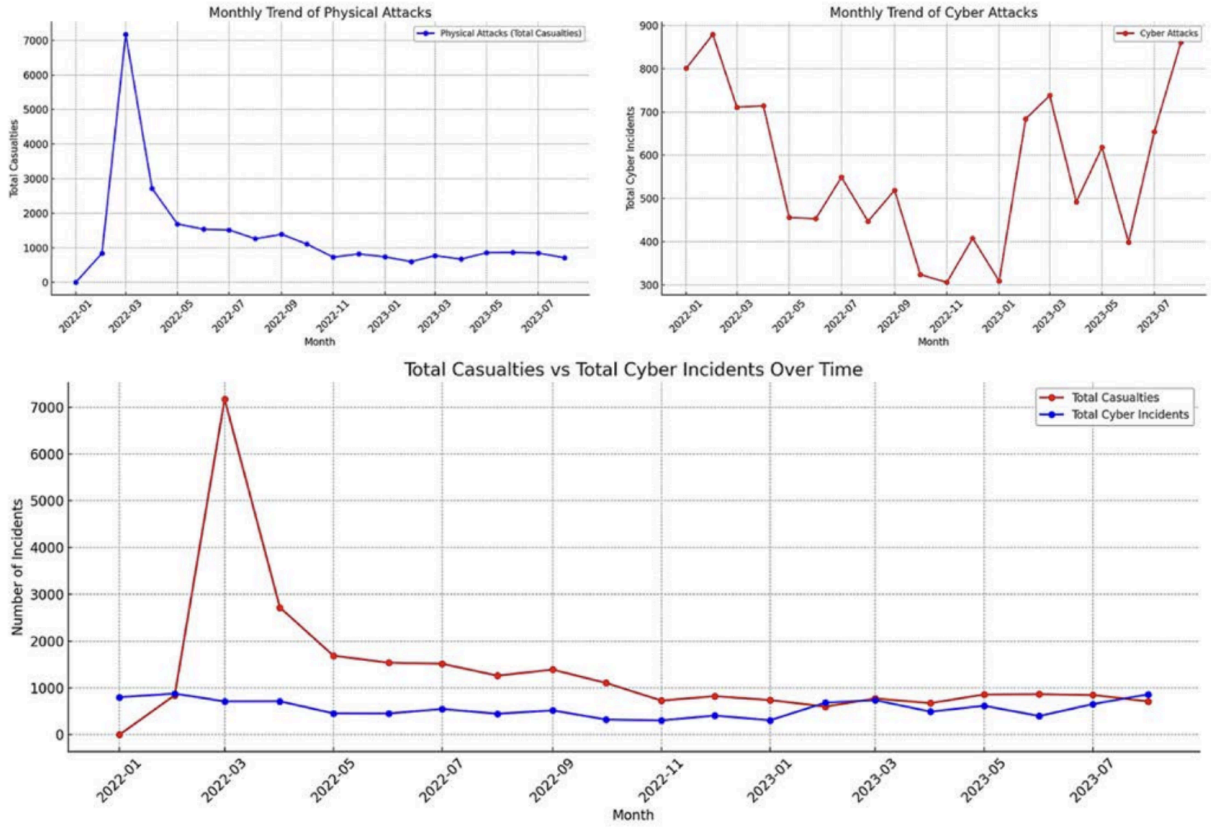
[318] News, T.H. (2024). *Pro-Ukrainian Hackers Strike Russian State TV on Putin's Birthday*. [online] The Hacker News.

[319] Knack, A., Kam, Y., Syn, H. and Tam, K. (2024). *Enhancing the Cyber Resilience of Offshore Wind*. The Alan Turing Institute.

[320] Fierro, C.D. and Dwyer, J. (2022). *Caddywiper malware targeting Ukrainian organizations*. [online] Ibm.com.

Comparing physical and cyber-based attacks over time may provide the most convincing evidence of this war's hybrid nature. After the first few months of the invasion, there was a decline in kinetic violence, but cyber incidents continued to be high and even increased in late 2023.

Figure 9: Initial Approximation of Physical vs Cyber Attack



Source: CYBER DIIA. (2024). A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience A comprehensive review.

Even as traditional battlefield activity stalled, cyberspace continued to be a primary front of aggression, as shown in Figure 9. This difference indicates that cyber operations are now a continuous, independent form of strategic pressure, rather than merely a supplement to war. This pattern indicates that Russia's use of digital warfare persisted into 2024 and beyond; in fact,

Ukraine experienced a sharp rise in cyberattacks in 2024, with a total of 4,315 incidents. Compared to the 2,541 incidents that were reported in 2023, this represents a 69.8% increase[321].
All of this demonstrates that cyberattacks during the Russian hybrid war in 2022 are not discrete technological tactics, but rather fundamental elements of strategic warfare deeply integrated into Russia's hybrid military doctrine.

3.1.4. The acceleration of NATO/EU frameworks integration

Everything stated in the above section explains the acceleration of NATO and EU cybersecurity framework integration in Ukraine. Ukraine received significant levels of political, operational, and technical support as it transitioned from being a strategic partner to a quasi-integrated member. Adopting Euro-Atlantic standards, deepening the institutionalisation of common practices, and expediting Ukraine's legislative, strategic, and technological alignment with NATO and the EU were all made possible by this support, which went beyond ad hoc aid.
The two organisations quickly mobilised after hostilities broke out. Through its Cyber Defence Trust Fund and C4 Trust Fund, established after 2014, NATO had already started collaborating with Ukraine. Initially, these programs offered software and critical infrastructure support for government systems. But after 2022, this support was increased. The National Police and Ukrainian Armed Forces established cybersecurity centres, which were linked to a nationwide network of situational awareness and response units. In order to facilitate long-term technological cooperation, NATO's Communications and Information Agency (NCIA) concurrently extended its Memorandum of Understanding with Ukraine in January 2022[322].
The EU deployed the Cyber Rapid Response Teams (CRRTs) under the Permanent Structured Cooperation (PESCO) framework. This was the first operational deployment of CRRTs in a live conflict. The deployment process began with a formal request from Ukraine in February 2022 and was approved by the CRRT Council, with Lithuania assuming leadership of the multinational team. Composed of cyber experts from six EU states, the CRRT provided real-time support in identifying vulnerabilities, mitigating threats, and securing critical infrastructure[323].

[321] Oleksii Artemchuk (2025). *Number of cyberattacks on Ukraine increased by 70% in past year*. [online] Ukrainska Pravda.
[322] Costigan , S.S. and Hennessy, M.A. (2024). *HYBRID THREATS AND HYBRID WARFARE REFERENCE CURRICULUM*. [online] *NATO Headquarters Brussels*.
[323]eda.europa.eu. (2022). *Activation of first capability developed under PESCO points to strength of cooperation in cyber defence*.

This was a turning point in EU cyber crisis management, as it involved both virtual and on-site operations within an active war zone[324]. In one of the earliest signs of deepening operational trust, the EU's High Representative publicly pledged cyber support to Ukraine following the coordinated cyberattack of January 14, 2022, which disabled the websites of several ministries[325]. On February 18, Ukraine formally requested CRRT deployment, and by February 22, the Council approved activation. Though the invasion began two days later, halting physical deployment, the EU maintained remote cyber defence coordination and threat monitoring, marking the first wartime operationalisation of the CRRT mechanism[326].

In addition to providing immediate aid, the EU announced a €29 million package to strengthen Ukraine's cyber capabilities. Of this, €19 million was allocated to long-term digital transformation, and €10 million supported immediate cybersecurity infrastructure upgrades[327]. Ukraine's shift to cloud-based services and robust digital systems was made easier with the help of organisations like the Estonian e-Governance Academy. To address both emergency assistance and long-term harmonisation with the NIS2 Directive, the Cyber Resilience Act, and the Cyber Solidarity Act, the EU also expanded its Cyber Dialogue with Ukraine, which has been conducted regularly since 2021. Harmonisation of laws and regulations was a key element of this integration. Ukraine brought its cybersecurity, e-services, and telecommunications laws up to date with those of the EU[328]. Ukraine's 2021 Cybersecurity Strategy was revised to align more closely with EU standards and to support interoperability with NATO frameworks, reflecting the country's broader Euro-Atlantic integration goals. The Annual National Programs (ANPs) continued to serve as the model for alignment with NATO, including specific targets related to military-civil cyber cooperation, internal cyber audits, and professional training[329].

A significant step towards Ukraine's integration into the Euro-Atlantic cyber defence community was taken in May 2023 when it formally joined the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. As a result of this membership, Ukraine was able to

---

[324] I. Fyshchuk "Stronger together? EU support for Ukrainian local authorities facing cyber attacks (2022–2023)," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190344

[325]Council of the EU (2022). *Ukraine: Declaration by the High Representative on behalf of the European Union on the cyberattack against Ukraine*. [online] www.consilium.europa.eu.

[326]Fyshchuk "Stronger together? EU support for Ukrainian local authorities facing cyber attacks (2022–2023)," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190344

[327]EEAS Press Team (2022). *Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue | EEAS Website*. [online] www.eeas.europa.eu.

[328] *Ibidem.*

[329]Head of the Office of the President of Ukraine A. Yermak (2024). *Cybersecurity Strategy of Ukraine | Digital Watch Observatory*. [online] Digital Watch Observatory.

participate in the largest live-fire cyber defence simulation in the world, Locked Shields 2024, where Ukrainian teams collaborated with international experts to enhance their coordination, incident response, and cyber forensics capabilities. Through this partnership, Ukraine benefits from the CCDCOE's structured frameworks for research and policy development while also contributing invaluable operational experience[330].

To strengthen collective cyber defence and assist national mitigation efforts against major cyber threats, NATO introduced the Virtual Cyber Incident Support Capability (VCISC) at the 2023 Vilnius Summit. Such efforts to improve cyber resilience are beneficial to Ukraine, a close NATO partner. By participating in the High-Level Dialogue on Innovation and Disruptive Technologies that same year, Ukraine strengthened its partnership with NATO by focusing on developing innovation ecosystems for both commercial and defence applications. In support of these initiatives, Ukraine created BRAVE1, a government-sponsored defence technology accelerator. By the middle of 2023, some 400 projects had been registered, with almost half of them undergoing military testing. This strengthened Ukraine's defence innovation and integration with Euro-Atlantic security frameworks[331].

A significant step in Ukraine's NATO integration was the establishment of the NATO-Ukraine Council (NUC) at the 2023 NATO Summit in Vilnius, which replaced the NATO-Ukraine Commission. With decisions decided by consensus, this new framework enables Ukraine to participate on an equal basis with all NATO members. NATO's commitment to Ukraine's political and military integration is reflected in the Council format, which enhances the ability to conduct rapid consultations during emergencies. Furthermore, the NATO Representation to Ukraine (NRU) remains an essential advisory organisation for aid coordination and strategic communication in Kyiv[332].

The EU and NATO also improved their Structured Dialogue on Resilience in terms of strategic coordination, citing Ukraine's defence of its vital infrastructure as an example of future civil-military cooperation. To coordinate cyber operations, exchange best practices, and synchronise legislation, this platform established the EU-NATO-Ukraine Cyber Dialogue, a trilateral format. The Joint EU-NATO Taskforce on Critical Infrastructure, established in March 2023, created shared threat assessments and scenario-based planning initiatives and strengthened

[330]Visitukraine.today. (2022). *Ukraine to be accepted as a Contributing Participant to NATO CCDCOE*. [online]
[331] NATO (2019). *Relations with Ukraine*. [online] NATO.
[332] NATO (2023). NATO-Ukraine Commission (1997-2023). [online] NATO.

these trilateral efforts[333]. Ukraine's real-world wartime experience influenced joint EU-NATO scenario planning within the Structured Dialogue framework and acted as a template for civil-military cooperation in protecting vital infrastructure.

By 2024, Ukraine was preparing to participate in NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund, initiatives designed to support dual-use and emerging technology startups. This move underscored Ukraine's deeper integration into the transatlantic defence-industrial network. Beyond receiving aid, Ukraine has actively contributed to shaping EU and NATO cyber doctrines, particularly through its experiences in rapid mobilisation, fostering public-private partnerships, and leveraging cyber volunteer forces, such as the IT Army. Ukrainian cybersecurity experts have also participated in workshops and training events on implementing the NIS2 Directive, organised by ENISA, thereby reinforcing Ukraine's alignment with EU cybersecurity governance. Furthermore, following the EU-Ukraine joint security commitments of June 2024, steps have been taken to facilitate Ukraine's participation in selected PESCO projects, further deepening operational and legislative integration[334].

A notable example of institutional change during a war is the integration of NATO and EU cybersecurity frameworks into Ukraine's digital and defence architecture. The EU Advisory Mission (EUAM), which provided Ukrainian ministries with institutional mentoring, legal expertise, and cyber policy advice, helped facilitate this transition on the ground. Additionally, the mission supported training in legislative draughting, public-sector cybersecurity planning, and strategic digital communication[335].

Although Ukraine's operational, legal, and technological integration into both frameworks has already occurred, full membership in NATO or the EU is still a long-term political process.

The NATO Madrid Summit in June 2022 served as the initial anchor for this trajectory, during which Allied leaders formally committed to supporting Ukraine's cyber resilience by allocating resources to safeguard communication networks, improve detection systems, and promote doctrinal alignment with NATO's cyber defence posture.

---

[333] Shelest H. - Omelianenko V. (2023). Policy Paper. EU, NATO and Ukraine. Dream Team or a Triangle. Ukrainian Prism.

[334] Defence Industry Europe (2024). *Council of the European Union approves PESCO Strategic Review*. [online] Defence Industry Europe.

[335] European Union External Action (2024). *Strengthening Cybersecurity Through Cross-Border Cooperation: Insights from Bucharest and Ivano-Frankivsk — EUAM Ukraine*. [online] EUAM Ukraine.

The cyber front of Ukraine is now a shared transatlantic and European security frontier. Importantly, compliance with NATO security principles and EU directives was already anticipated in Ukraine's 2021 cybersecurity strategy. Early harmonisation accelerated institutional preparedness, legal compatibility, and technological interoperability with Euro-Atlantic partners, enabling Ukraine to integrate support mechanisms when war began.

3.2. Case Studies of Russian Cyberattacks on Critical Infrastructure

The critical cyberattacks against Ukraine's energy sector in December 2015 and December 2016 are thoroughly examined in this section of my thesis. These incidents have several uses in helping me unpack the research puzzle, such as providing a technical and historical assessment of Ukraine's early cyber vulnerabilities prior to NATO and EU aid. Because Ukraine creates baseline assessments to track its increasing resilience following the expansion of the Euro-Atlantic partnership, the research examines these attacks to demonstrate how its cybersecurity response strategies have evolved in response to external threats.

It is impossible to overestimate the strategic importance of energy infrastructure in contemporary statecraft. The stability and resilience of a nation's energy systems, which form the basis of its industrial, military, and civilian endeavours, are closely related to its national security. Power plants, transmission lines, substations, and distribution centres make up energy grids, which are vital lifelines rather than just technical systems. Due to their deep integration with cyber-physical operations in an increasingly digitalised world, these systems are vulnerable to cyberattacks. The relationship between critical infrastructure and cyberwarfare has never been more evident than in Ukraine. Important turning points in the history of cyberwarfare were the December 23, 2015, and December 17, 2016, cyberattacks on Ukraine's energy sector. These were the first known successful instances where a cyberattack led to a coordinated and deliberate disruption of a national power grid.

The December 2015 Cyberattack

Three regional electricity distribution companies were the targets of a well-planned cyberattack on December 23, 2015, during the busiest holiday season in Ukraine: Prykarpattyaoblenergo in

Ivano-Frankivsk, Kyivoblenergo in the Kyiv region, and Chernivtsioblenergo in Chernivtsi. The attack resulted in widespread power outages that affected approximately 230,000 people for periods ranging from one to six hours[336]. This event was the first publicly acknowledged successful disruption of a power grid cyberattack. It is generally accepted that Sandworm, a Russian state-sponsored threat actor, was the main attacker.

The attackers infiltrated the target companies through spear-phishing campaigns that deployed the BlackEnergy 3 malware, a modular and sophisticated toolkit designed for cyber espionage and sabotage. Employees received emails that appeared to be from Ukrainian authorities, encouraging them to open documents embedded with malicious macros. Once opened, these macros downloaded and installed the malware, granting the attackers remote access to the corporate networks[337].

After months of reconnaissance and privilege escalation, Sandworm successfully obtained administrative access to Supervisory Control and Data Acquisition (SCADA) systems. These systems are critical to the real-time control and monitoring of electrical grid operations. Using stolen credentials and virtual private network (VPN) connections, the attackers gained remote access to the control centres. At approximately 3:35 p.m., the attack was launched in a synchronised manner across all three energy companies. Attackers took manual control of operator interfaces and remotely opened circuit breakers at about 30 substations, servicing the Ivano-Frankivsk region[338].

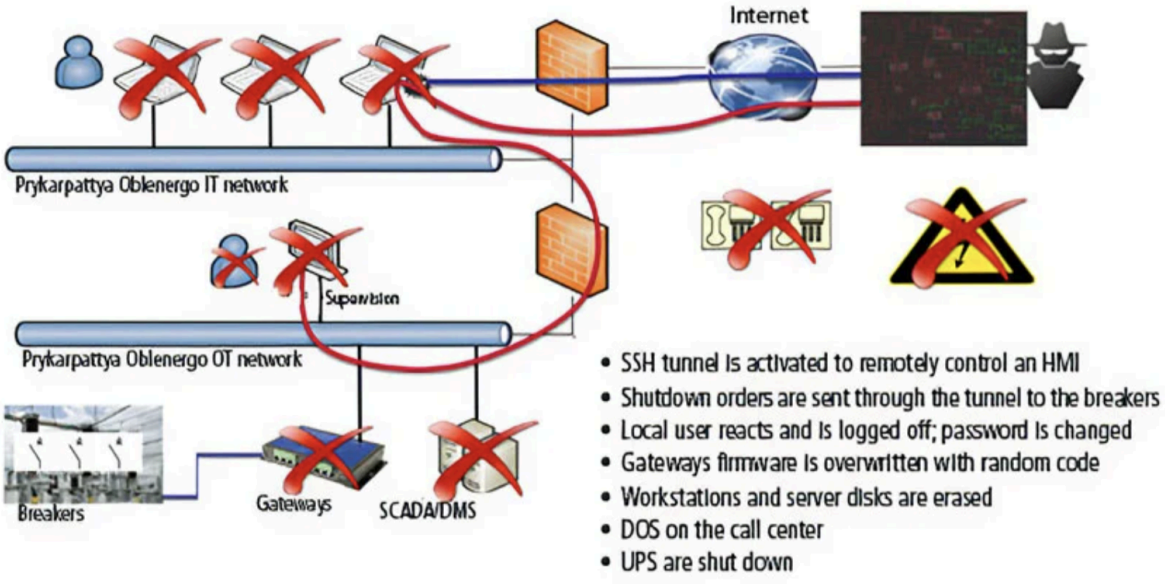
The sophistication of the attack rests in its multi-pronged methodology. First, SCADA systems were exploited to open breakers, cutting power to hundreds of thousands of people. Second, attackers disabled the uninterruptible power supplies (UPS) meant to maintain operational continuity at the control centres, thereby sending them into darkness and chaos. Third, they disabled or "bricked" serial-to-Ethernet converters at substations, thereby halting remote restoration efforts and forcing manual interventions. Fourth, a denial-of-service (DoS) campaign targeted the customer service phone lines of the energy companies, preventing affected citizens from obtaining information. Finally, the attackers deployed KillDisk malware to wipe data from the affected systems and corrupt the master boot records, rendering them unusable[339].

---

[336] CISA (2021). *Cyber-Attack Against Ukrainian Critical Infrastructure*. [online] Cybersecurity and Infrastructure Security Agency.
[337] *Ibidem.*
[338] Don, J. (2017). *Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack*. [online] blog.isa.org.
[339] *Ibidem.*

The psychological impact of this attack, rather than the extent of its damage, set it apart from earlier cyberattacks. Videos recovered from the scene demonstrated the attackers' control by displaying cursors moving across operator screens and braking devices in real time. Figure 10 below, which recreates the third and last phase of the cyberattack on Prykarpattyaoblenergo's infrastructure, illustrates the sequence of events.

Figure 10: Representation of the attacker taking control of the SCADA interface, locking out the operator.



Source: Don, J. (2017). *Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack*. [online] blog.isa.org.

The attack was more effective because it was planned for a seasonal holiday when staffing was lower. The use of KillDisk, which erased data essential to service restoration and damaged Ukrainian officials' trust in the reliability of their infrastructure, exacerbated the psychological warfare element even more.

Although the blackout lasted only a few hours, it had a significant impact. It demonstrated that cyber operations could extend beyond espionage and into the realm of sabotage, with real-world physical consequences. Furthermore, the attack demonstrated Russia's cyber capabilities clearly and concisely. The limited scope suggests a calibrated message rather than an aggressive strike, even though it could have caused more damage. Analysts argue that this restraint was strategic,

an exhibition of power intended to warn Ukraine and its Western allies about the sophistication and potential of Russian cyber warfare.

The December 2016 Cyberattack

On December 17, 2016, almost a year after the 2015 incident, Ukraine was the target of another cyberattack, this time against the Pivnichna 330kV transmission-level substation outside Kyiv. The attack was equally significant in terms of its technical innovation and implications, even though the affected area and population were smaller, roughly one-fifth of Kyiv's nighttime electricity load. A new and more sophisticated malware strain, called Industroyer or CRASHOVERRIDE, was used by the group responsible for this attack, which is generally attributed to Electrum, a subgroup or extension of Sandworm.

Industroyer was specifically designed for use against electric grid systems, in contrast to its predecessor. This degree of specialisation represented a breakthrough in cyberweapon design since the malware was able to communicate directly with hardware devices without depending on the human-machine interfaces (HMIs) that operators usually use. It achieved this by leveraging industrial communication protocols. The attackers were able to give circuit breakers and other field devices valid commands thanks to this capability[340].

The attack consisted of three main stages. Initially, all the circuit breakers at the Pivnichna substation were opened by the malware, resulting in an instantaneous power outage. Second, a wiper component akin to KillDisk was launched by the attackers, disabling important IT infrastructure components at the station, such as supervisory systems and HMIs. Third, they tried to turn off the SIPROTEC protective relays, which trip circuits in the event of anomalies to guarantee operational safety[341]. The attempt demonstrated a clear intent to cause long-term, potentially irreparable physical damage, despite the relays not being completely disabled due to an IP targeting misconfiguration.

Analysts speculate that this attack had more ambitious goals, even though the 2016 blackout was restored faster than the one the year before. By focusing on protective relays, the attackers aimed to hinder the ability to safely recover, in addition to simply disrupting service. Re-energising the

[340] Cherepanov, A. (2016b). "The Rise of Telebots: Analyzing Disruptive KillDisk Attacks." WeLiveSecurity, December 13, 2016.

[341] CISA. (2021a). Cybersecurity and Infrastructure Security Agency. "Cyber-Attack against Ukrainian Critical Infrastructure: CISA." Cybersecurity and Infrastructure Security Agency CISA.

station could have caused severe equipment damage or even injuries to personnel if the relays had been successfully disabled[342].

Russia's cyber strategy shifted from disruption to possible destruction with the deployment of Industroyer. Industroyer was designed to avoid many of the steps that BlackEnergy required, including months of reconnaissance and lateral movement within corporate networks. It demonstrated the growing sophistication of Russian cyber operations by being practical, modular, and capable of being executed automatically. Furthermore, by embedding the malware with time-delayed execution features, the attackers minimised their risk of detection and maximised operational impact.

One interpretation of the 2016 attack is that it was either a real-world training exercise or a demonstration of enhanced capability. Once again, the close temporal proximity to the 2015 incident and the holiday season suggest a purposeful psychological element. The attackers reaffirmed their persistent presence and willingness to attack by demonstrating that even more robust defences could be evaded. Despite the attack's failure to produce disastrous results, analysts have pointed out that it had considerable strategic and symbolic significance[343].

The combined cyberattacks on Ukraine's energy sector in 2015 and 2016 demonstrate how state-sponsored cyberwarfare can precisely and psychologically target vital infrastructure. The strategic logic of hybrid warfare, in which cyber operations serve as force multipliers, highlights the vulnerabilities of legacy systems and the perils of inadequate cybersecurity protocols. These incidents, which were part of the larger geopolitical conflict between Russia and Ukraine, were political signalling rather than technical exploits. The following section will examine Ukraine's response strategies, institutional flaws, and the development of its cyber resilience since 2016, with a particular focus on its growing integration with the European Union and NATO.

3.2.1. Early vulnerabilities before deeper integration

The cyberattacks on Ukraine's power grid in 2015 and 2016 exposed systemic weaknesses in the country's institutional structure, cybersecurity posture, and national infrastructure in addition to

[342]Cerf E. (2024). Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world. UC SANTA CRUZ

[343] *Ibidem.*

the adversary's technical prowess[344]. Ukraine's ability to detect, identify, and respond to sophisticated state-sponsored cyber threats was also constrained at the time, as was its capacity to integrate into Western defence and security frameworks. The attacks revealed a nation that was still heavily dependent on outdated infrastructure, lacked well-coordinated national defence systems, and was just starting to build up the institutional knowledge required to avoid such highly skilled attacks[345].

The design of Ukraine's electrical grid was one of its flaws. A large portion of the infrastructure was Soviet-made and was still heavily centralised, poorly documented, and intertwined with antiquated and inadequately divided digital systems. Many pieces of industrial control equipment, such as SCADA systems and remote access tools like Radmin, were designed with remote access in mind but lacked modern cybersecurity safeguards[346]. Once initial access was gained, it became easier for attackers to move laterally across the network. Most notably, there was little to no separation between the operational technology (OT) networks that oversaw grid infrastructure and the information technology (IT) networks used by corporate management. The lack of network segmentation offered a simple bridge from phishing-based intrusions on the business side to sabotage of industrial controls on the operational side[347].

Procedural and organisational flaws complemented technical vulnerabilities. Utilities functioned without robust internal response protocols for coordinated cyberattacks, and staff members received little cybersecurity training. Staff members' lack of training in even the most fundamental aspects of cyber hygiene contributed to the success of social engineering techniques like phishing emails that were designed to look like official correspondence from government ministries[348]. Neither a culture of caution when opening attachments or enabling macros nor standard procedures for authenticating suspicious documents existed. Furthermore, the absence of identity and access management controls allowed credential-gaining intruders to escalate privileges and assume the identities of authorised users without setting off alarms. The absence

[344] Luhn, A. (2015). "Crimea Declares State of Emergency after Power Lines Attacked." The Guardian. Guardian News and Media.

[345]Lee, R. M, Assante, m. J., & Conway, T. (2018). "Analysis of the Cyber Attack on the Ukrainian Power Grid," Electricity Information Sharing and Analysis Center, pp. 1- 29, 24-25.

[346]Prokip, A. (2025). *Ukraine's Energy Sector: Resilience After Three Years of Full-Scale War*. [online] Wilson Center.

[347] *Ibidem.*

[348]Borychenko, O.et al.. (2024). CYBERSECURITY IN THE ENERGY INDUSTRY OF UKRAINE: PROTECTION MEASURES AND CHALLENGES IN THE CONTEXT OF ENERGY SECURITY. *Revista Gestão & Tecnologia*, *24*(4), 67-90.

of multi-factor authentication, the presence of vulnerable protocols like NTLM, and the failure to use application whitelisting all provided intruders easy paths for further penetration[349].

By the time the intrusions started in 2015 and 2016, Ukraine's ability to react was severely limited. The forensic and investigative response was limited even though power was restored in a matter of hours. For instance, the full scope of the intrusion was not immediately apparent in the 2015 attack, which left dozens of systems damaged or destroyed by KillDisk malware[350]. Insufficient training and equipment prevented Ukrainian incident response teams from conducting comprehensive digital forensics independently. The nation was heavily dependent on outside assistance, specifically from the United States, which included collaboration with the FBI, ICS-CERT, and the Department of Energy. While this global coordination was highly beneficial, it also indicated Ukraine's dependence on foreign expertise to even understand what had taken place, let alone create countermeasures[351].

The ad hoc response was further hampered by the lack of a comprehensive national cybersecurity strategy. The Computer Emergency Response Team of Ukraine, or CERT-UA, functioned without a clear legal mandate or sufficient personnel to facilitate coordination among impacted businesses, government agencies, and foreign partners[352]. CERT-UA responded to the attacks quickly and cooperatively, but it lacked the power to impose defensive measures on critical infrastructure sectors or mandate best practices. Furthermore, lessons learnt were only gradually applied because utilities lacked a shared threat-intelligence platform and reporting procedure. Each business reacted on its own, frequently, without knowing what had happened at the others. The attackers were able to reuse tactics against numerous targets without hindrance due to this fragmentation[353].

Ukraine had political, structural, weaknesses along with technical ones. The country's vulnerability was increased by years of underinvestment in cybersecurity, a lack of strategic prioritisation, and a continued reliance on Russian-made hardware and software. Since many of the grid's components were still based on Russian technology, it was more likely that the attackers were familiar with the systems they were targeting. Furthermore, the timing of the

[349] Shehod, A. (2016). Ukraine power grid cyberattack and US susceptibility: Cybersecurity implications of smart grid advancements in the US. *Cybersecurity Interdisciplinary Systems Laboratory, MIT*, *22*, 2016-22.

[350] Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2016). The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE transactions on power systems*, *32*(4), 3317-3318.

[351] *Ibidem.*

[352] Kostyuk, N., & Geers, K. (2015). Ukraine: A Cyber Safe Haven?. *Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence*, 113-122.

[353] *Ibidem.*

attacks, during the winter holidays, emphasised yet another serious flaw: a lack of operational redundancy. The attack itself and subsequent telephone denial-of-service campaigns disrupted internal communications, escalation protocols were unclear, and there were only skeleton staff on duty[354].

Notwithstanding these difficulties, the attacks sparked a positive change in public perception. They served as a warning to Ukrainian policymakers that cybersecurity and energy security were inextricably linked, and that until significant reforms were implemented, foreign attackers would continue to exploit these weaknesses. Interest in Western approaches to cybersecurity governance, particularly those supported by NATO and the European Union, surged in the wake of the attack. In order to conduct joint exercises and adopt policy tools like the NIST Cybersecurity Framework and elements of the EU's developing cyber defence doctrine, Ukrainian officials started to collaborate with foreign partners more frequently[355].

However, due to institutional fragmentation and legacy infrastructure, the nation's response to the events of 2015 and 2016 was mainly reactive in the short term. There were no formal national contingency plans in place to address cyberattacks on critical infrastructure. Standardised playbooks and scenario-driven drills were absent from the impacted companies. For instance, because the systems had been rendered inoperable, operators had to manually visit distant substations to restore electricity, usually without the use of digital monitoring. The fact that restoration required the least amount of human intervention suggests that automation fallbacks and continuity of operations planning are lacking. Furthermore, no coordinated communication plan was in place to notify the public or mitigate the psychological effects of the blackout.

As it turned out, human ingenuity rather than systemic readiness was more responsible for Ukraine's resilience during these years. It is not the strength of the national cyber defence apparatus, but rather the creativity and commitment of local engineers, that enabled power to be restored in hours rather than days. From an institutional perspective, the response revealed Ukraine's lack of readiness for coordinated, nation-state-level cyberattacks.

Therefore, Ukraine's response to the attacks in 2015 and 2016 was one of quick physical reconstruction but little strategic foresight. Many of the lessons learnt were only made into

[354] *Ibidem.*

[355] Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*, *6*.

policy after additional attacks and sustained international pressure, and the vulnerabilities revealed during those years were not immediately fixed. These early failures, however, played a foundational role in shaping the nation's long-term approach toward cyber resilience, demonstrating the cost of delay and the necessity of integration within collective defence frameworks.

3.2.2. Cyberattacks during Russian Hybrid warfare

This section examines three major cyber incidents, two of which occurred in 2022 and one in 2024, that collectively illustrate how cyber threats to Ukraine's energy sector are evolving. The following case studies demonstrate how the energy sector has remained a crucial conduit through which adversaries try to topple the government, disrupt critical services, and cause psychological harm to civilians. This will be accomplished by examining the malware employed, operational processes, and broader geopolitical implications.

The main target of a string of extremely sophisticated cyberattacks carried out in 2022 against the backdrop of the Russian invasion was Ukraine's energy sector[356]. The targeted attacks on vital infrastructure and the operational complexity of Russian state-sponsored actors, most notably the Sandworm group associated with the Russian military intelligence agency GRU, are demonstrated by two distinct incidents that took place in April and October. The energy sector is both a symbolic and strategic target of these attacks, which represent a continuation and a major escalation of Russia's cyberwarfare strategy[357].

High-voltage electrical substations in Ukraine were the target of the first attack, which was stopped in early April 2022. The attack was later revealed to be one of the most sophisticated cyberattacks known to have occurred during the ongoing conflict by Ukrainian cybersecurity authorities[358]. According to forensic analysis, the attackers had been infiltrating the energy company's networks since February 2022, triggering a prolonged reconnaissance and payload development phase. Industroyer2, the successor to the popular Industroyer malware used in the 2016 Kyiv blackout, was the foundation of the attack. A specially designed malware for

[356] Lilly, B., & Cheravitch, J. (2020, May). The past, present, and future of Russia's cyber strategy and forces. In *2020 12th International Conference on Cyber Conflict (CyCon)* (Vol. 1300, pp. 129-155). IEEE.
[357] Warren, M., Štitilis, D., & Laurinaitis, M. (2023). The impact of Russian cyber attackers within the Ukraine situation. *Journal of Information Warfare*, *22*(1), 88-107.
[358] Pearson, J. (2023). Russian spies behind cyber attack on Ukraine power grid in 2022 - researchers. *Reuters*. [online] 9 Nov.

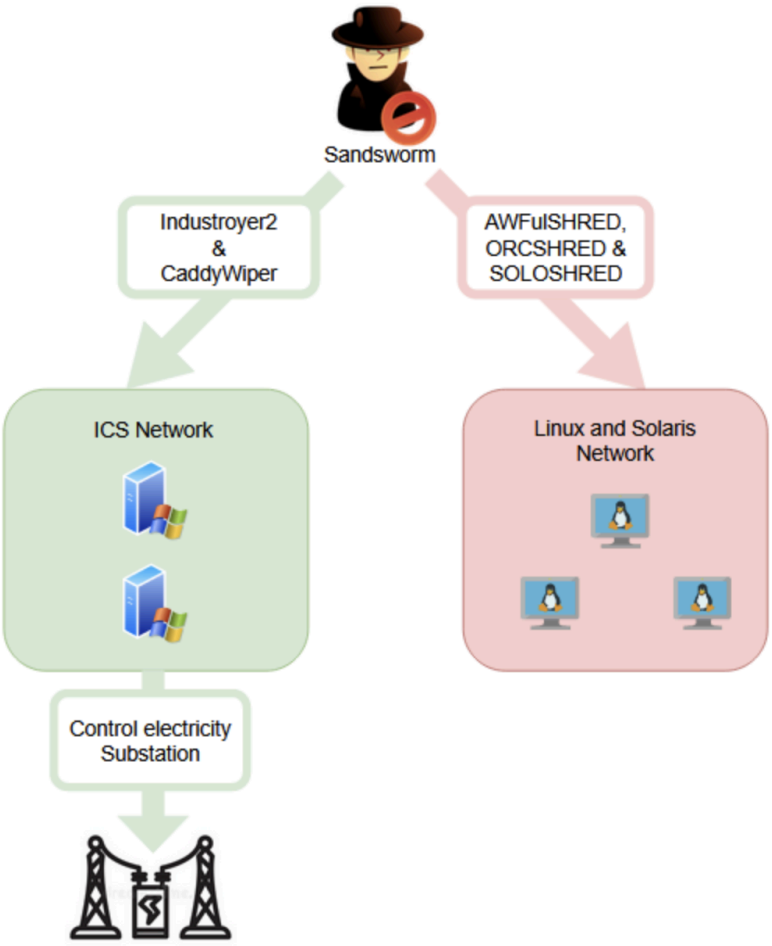
Industrial Control Systems (ICS), Industroyer2 was created to interfere with substation protection relays and circuit breakers[359]. It is capable of sending direct commands to industrial equipment by using the IEC 104 protocol, a standard communication protocol built into power grid systems. In addition to being able to function as a logic bomb that is preloaded to attack at a specific time, Industroyer2 stands out from its predecessor due to its high degree of customisation. The version used in this attack was scheduled to launch on April 8, 2022, at 16:10 UTC, a time chosen to coincide with a Friday when civilian activity is at its highest.

If the attack had been successful, it could have cut off electricity to about two million people, severely impairing Ukraine's capacity to continue daily operations, communication, and military supplies. Furthermore, a group of malicious programs were installed on Industroyer2 through the coordinated use of several Linux-based wipers, such as CaddyWiper, OrcShred, SoloShred, and AwfulShred, which were designed to destroy logs, data, and make system recovery more difficult[360].

[359]Proska , K. et al (2023). *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*. [online] Google Cloud Blog.

[360] Ganesh PAJANI and Paul PEIX (2022). *Industroyer 2 : the Russian Cyberattack on Ukraine Infrastructure*. [online] Headmind Partners.

Figure 11: Sandworm's coordinated cyberattack on Ukraine's energy sector (April 2022)



Source: Ganesh PAJANI and Paul PEIX (2022). *Industroyer 2 : the Russian Cyberattack on Ukraine Infrastructure*. [online] Headmind Partners.

The above scheme exemplifies Sandworm's two-phase approach used in the April 2022 operation. The operation aimed to paralyse Ukraine's recovery and forensic capabilities in addition to disrupting the grid by using Industroyer2 and CaddyWiper to target the ICS environment that controls electricity substations and multiple wipers to attack administrative Linux systems. Fortunately, CERT-UA, ESET, and Microsoft collaborated to successfully halt the attack. Their prompt action not only prevented the impending threat but also demonstrated Ukraine's increasing cybersecurity proficiency, particularly in identifying and thwarting sophisticated, modular, and covert malware explicitly designed for SCADA systems[361].

[361] Pearson, J. (2022). Ukraine says it thwarted Russian cyberattack on electricity grid. *Reuters*. [online] 12 Apr.

The second attack, on the other hand, was successful and took place between October 10 and 12, 2022. In this instance, Sandworm successfully compromised a Ukrainian electrical substation, conducting a multi-event cyber-physical attack. The intrusion started with the compromise of a server exposed to the internet, where Sandworm deployed a Neo-REGEORG webshell in June 2022. Over the following months, the hackers conducted lateral movement across the network via GOGETTER, a tunneling application, and accessed the hypervisor that controlled the SCADA system[362].

In this case, the use of so-called Living off the Land (LotL) tactics meant that attackers leveraged legitimate software in unintended ways, which allowed them to remain undetected and accelerate deployment. The assault resulted in a surprise power outage, a cyber-physical interference that was strategically synchronised with a wave of Russian missile strikes on energy infrastructure throughout Ukraine[363]. The convergence of these two aspects, cyber and kinetic, demonstrates the integration of cyber operations within comprehensive military initiatives.

Two days later, on October 12, Sandworm deployed a new variant of CADDYWIPER in the same IT system of an organisation, leveraging Group Policy Objects (GPOs) for distribution and execution of the wiper. The malware was aimed at permanently deleting files and mapped drives, and potentially wipe forensic evidence of OT compromise. Although the SCADA system was not targeted directly, the utilisation of CADDYWIPER is a calculated effort at extending disruption, hindering administrative procedures, and precluding timely incident management[364].

These two cyberattacks demonstrate that, within the larger context of hybrid warfare, Ukraine's energy infrastructure was a top target.. Even though it had been stopped, the April attack showed the precision, customisation, and strategic timing that define Sandworm's operations. However, the October incident demonstrated the operational maturity of Russia's cyber troops, showcasing their ability to conduct cyber-physical sabotage, integrate information technology and operational technology environments, and coordinate attacks with military campaigns.

[362] Fyshchuk, I., Noesgaard, M. S., & Nielsen, J. A. (2024). Managing cyberattacks in wartime: The case of Ukraine. *Public Administration Review*.
[363] Lewis, J. A. (2022). *Cyber war and Ukraine*. Center for Strategic and International Studies (CSIS).
[364] Adamov, A. RUSSIAN WIPERS IN THE CYBERWAR AGAINST UKRAINE.

The ongoing cyberwar against Ukraine's energy sector continued. I will focus on another attack that took place in January 2024. In addition to responding to persistent threats, the cyberattack introduces features that demonstrate how strategies and tools have evolved.

Lvivteploenergo, a city-owned energy utility that provides heat in the western Ukrainian city of Lviv, was the target of the attack. Over 600 buildings were left without heat for 48 hours during the winter due to the incident. The incident had significant strategic and symbolic importance, highlighting the susceptibility of civilian life to cyber-physical disruptions, despite being smaller in scope than earlier attacks against the national grid[365].

FrostyGoop, a previously undiscovered type of malware, was at the heart of this cyber intrusion. Since this malware is the first variant to be publicly documented as directly communicating with Industrial Control Systems (ICS) via the Modbus TCP protocol, it represents a significant milestone in terms of its functional features. Modbus, a protocol that is widely used in both contemporary and ageing industrial settings, has long been notorious for lacking built-in security features. However, before this incident, it had hardly ever been used in a way that resulted in such tangible and measurable impacts[366].

Analysts estimate that the attackers likely gained access as early as April 2023. The attackers remained undetected for the next few months, methodically gathering user credentials and extensively mapping the system. Although no concrete attribution has been proven, connections to the city power grid from Moscow-based IP addresses were observed in the run-up to the attack, suggesting potential ties to actors loyal to the Russian nation-state[367]. Ultimately, the malware was utilised to send malicious Modbus commands to ENCO controllers, which are devices that monitor boiler plant operations and heating substation modules. Due to inaccurate measurements and control system malfunctions brought on by the orders, the affected residents' access to heat and hot water was eventually cut off[368].

FrostyGoop differs from previous, more sophisticated ICS malware such as Industroyer2 or BlackEnergy, in that it is easy to use. Experts have noted that the ramifications are significant, despite their apparent simplicity. The malware serves as an example of how ICS operations can be impacted by even basic software, particularly in cases where systems are poorly segmented or

[365] Vasquez, C. (2024). *Simple 'FrostyGoop' malware responsible for turning off Ukrainians' heat in January attack*. [online] CyberScoop.
[366] *Ibidem.*
[367] Ribeiro, A. (2024). *Dragos details novel FrostyGoop ICS malware using Modbus TCP to disrupt OT operations worldwide*. [online] Industrial Cyber.
[368] *Ibidem.*

vulnerable. A cyberattack against Lvivteploenergo in January 2024 utilised FrostyGoop to disrupt heating services for over 600 apartment buildings in the Sykhiv district of Lviv, which is home to approximately 100,000 people. This incident shows how attackers can use little resources to cause public anxiety and distress.[369].

The attack was part of a broader wave of cyberattacks targeting Ukraine, which also included simultaneous assaults on the country's state oil and gas company and postal service. There is a pattern of these cyberattacks being coordinated with actual military operations, like drone and missile attacks against energy infrastructure, according to the Security Service of Ukraine (SBU) and other security experts. This integration demonstrates an evolved doctrine of operation that attempts to simultaneously saturate key systems from multiple perspectives. FrostyGoop's origin and deployment context strongly imply state sponsorship in pursuit of Russia's strategic objectives, specifically undermining Ukraine's resolve and resilience, although it is not attributed to a specific actor. Finally, the 2024 Lviv attack highlights the continued vulnerability of municipal and decentralised power infrastructures, despite the strengthening of national infrastructure. Large-scale, centralised blackout operations, like those in 2015 and 2022, are giving way to targeted, localised outages that are more difficult to predict and defend against. Furthermore, it highlights the growing risk posed by outdated protocols, such as Modbus, which are still widely used in critical infrastructure worldwide. The incident confirms that the energy sector remains a top target in cyber warfare, despite Ukraine's prompt and efficient response, which mitigated the outage and restored services within two days.

3.3. Comparative analysis

Despite their devastating effects, the attacks over the past ten years have tested Ukraine's institutional and digital defences. In addition to demonstrating increasing domestic capability, Ukraine's response has evolved from ad hoc recovery efforts in 2015 to coordinated, multifaceted mitigation efforts, as seen in 2024. This change is rooted in the country's growing integration with NATO and EU cybersecurity frameworks.

In the context of Euro-Atlantic aid, this section compares Ukraine's response to the five major cyberattacks in the energy sector previously discussed and measures how that response has

[369] Greenberg, A. (2024). *How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter*. [online] WIRED.

evolved over time. The objective is to critically evaluate whether Ukraine's resistance to Russian cyberattacks has changed in a measurable way as a result of this integration. This analysis reveals a trajectory of increasing institutional maturity and operational resilience in Ukraine's cyber defence strategy. In line with this thesis's core argument, each case provides empirical ground to assess how the integration of NATO and EU cybersecurity frameworks has influenced the effectiveness of Ukraine's response.

Wake-Up Calls: The 2015 and 2016 Cyberattacks

The cyberattacks in December 2015 and 2016 were crucial wake-up calls that revealed the extreme vulnerability of Ukraine's energy infrastructure, a large portion of which was built using antiquated designs from the Soviet era. Critical cyber hygiene flaws, including the lack of multi-factor authentication, inadequate internal response protocols, and unsegregated IT and OT environments, were highlighted by the 2015 attack in particular. Attackers were able to remotely shut down substations by manipulating SCADA systems, which required field technicians to restart them manually.

The institutional reaction was disjointed. Despite its urgency, CERT-UA lacked the resources and legal authority necessary to efficiently coordinate with other government agencies, independent energy providers, and foreign partners. Although outside aid from agencies such as the U.S. Department of Energy and ICS-CERT offered insightful information about the attacks, it also highlighted Ukraine's need for a centralised threat-sharing platform and a unified national cybersecurity strategy.

These events sparked a dramatic change in Ukraine's cybersecurity strategy, leading decision-makers to stop considering cyber defence as a separate technical problem and instead incorporate it into the larger national defence and energy policy frameworks[370].

Transformation Under Fire

The full-scale Russian invasion in 2022 unleashed a genuinely unprecedented ramp-up in the building of Ukraine's cyber defence. What had been a protracted effort to align the practices of

[370] 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 & Sustainability Issues*, *9*(3).

national institutions with NATO and EU norms became, nearly overnight, an existential imperative.

Nowhere was this more apparent than in the energy sector, where it was not only evident in Ukraine's improved ability to respond to incursions but also in the structure and coordination of its national cyber crisis management. One of the most advanced attacks ever recorded, the failed operation in April 2022, is telling evidence of that evolution. Industroyer2, a modular class of malware featuring logic bombs, was detected and neutralised before it could disable substations. This successful containment was the result of a complex web of domestic and international cooperation. CERT-UA did, in fact, partner with ESET and Microsoft to observe anomalies, analyse the malware, and issue advisories in mere hours. This response was understandably dissimilar from the disjointed response to the 2015 attack.

This represents a sharp departure from earlier piecemeal responses and affirms the central hypothesis of this thesis, that NATO and EU cybersecurity frameworks have had an impact on Ukraine's resilience to sophisticated Russian cyberattacks on key infrastructure[371]. The subsequent attack in October 2022, although partially successful, further demonstrated Ukraine's enhanced ability to handle cyber-physical convergence. The attack used sophisticated "living off the land" techniques to attack MicroSCADA systems and resulted in a temporary blackout. Ukraine, nevertheless, conducted real-time forensics, tracked the attackers' lateral movement, and isolated the malware.

The Virtual Cyber Incident Support Capability (VCISC) of NATO, the inclusion of Ukraine in the Cooperative Cyber Defence Centre of Excellence and Locked Shields exercise process (UN-classified), provided a planned, exercised, coordinated, and interoperable response process with Allied systems. Although they were not ultimately used due to the invasion, the EU's February 2022 activation of Cyber Rapid Response Teams represented a significant step forward for European cyber crisis management. Furthermore, Ukraine's long-term digital transformation initiatives, as well as its immediate cybersecurity infrastructure upgrades, were made possible by the EU's €29 million support package. All of these changes represent Ukraine's transition from a passive recipient of cyber assistance to an active member of a multilateral cyber governance framework, strengthening its defences against advanced cyber threats.

[371] *Ibidem.*

Expansion to Local Infrastructure: The 2024 FrostyGoop Attack

The FrostyGoop attack on municipal-scale energy infrastructure in January 2024 introduced a new dimension to Ukraine's cyber security challenges. In contrast to the nation-grid-focused operations from 2015 to 2022, FrostyGoop focused on a local heat supplier. The malware was simple but efficient; it took advantage of Modbus TCP, a legacy protocol that is still widely used in industry, to cut off the heat to more than 600 buildings for two winter days[372].

The Ukrainian response was prompt, accurate, and well-coordinated at the local level. Without escalation, national authorities could successfully detect malware, link the intrusion to IP addresses located in Moscow, and restore services. In addition to advanced technology, the attack shows an adaptable capacity for cyber resilience through readiness, efficient communication, and institutionally internalised practices. It also crucially illustrates how, in spite of the growing hardening of national systems, decentralised infrastructures still have inherent vulnerabilities.

The capacity to react quickly to minor disturbances, even in this municipal-scale setting, demonstrates that the resilience promoted by Euro-Atlantic integration extends beyond national infrastructure, a conclusion that supports the plausibility of the central hypothesis, suggesting a positive relationship between integration and resilience.

Even though cyberattacks were partially successful, Ukraine's cyber resilience has improved, thanks in large part to NATO and EU support. It is essential to contextualise these findings within the broader framework of hybrid warfare, as the majority of the attacks examined in this study were part of larger campaigns that included kinetic military strikes, physical sabotage, and missile attacks against the same infrastructure, rather than isolated cyber incidents. Concurrent threats have a compounding effect that makes attribution and containment more difficult, indicating that minor setbacks often mask significant defensive gains.

The ability of Ukraine to respond to such multifaceted pressures is a testament to its strength, cultivated under the most challenging circumstances, not a sign of weakness. This strength has its deep roots in Ukraine's growing integration into Euro-Atlantic cybersecurity frameworks.

[372] Silva, D. (2024). *FrostyGoop the New Addition to ICS Specific Malware – Cyber*. [online] Hawaii.edu.

Key Findings: Ukraine's Systemic Evolution in Cyber Resilience

Three broad and related trends emerge from an analysis of the five significant cyberattacks that have impacted Ukraine's energy infrastructure over the last decade, highlighting the nation's development of cyber resilience. These signify a systemic shift in Ukraine's cybersecurity posture rather than discrete enhancements. A distinct aspect of change, in strategy, partnerships, and integration, is captured by each theme.

The first theme relates to Ukraine's transition from improvisation to doctrine. Ukraine had to improvise its responses to attacks in the early stages of its cyber defence, mainly depending on the initiative of individuals working within institutional constraints. The attacks in 2015 and 2016 exposed significant systemic flaws and a deficiency in established protocols. The wartime revision of Ukraine's 2021 Cybersecurity Strategy, on the other hand, was the result of the country's development of a structured cybersecurity doctrine by 2022 that complied with NATO and EU standards. This framework integrated cyber defence into national security operations, defined escalation protocols, and clarified institutional roles[373]. Through coordinated procedures, Ukraine was able to anticipate and contain cyber threats, and respond more effectively as a result of this transition.

The second theme is the move from dependency to coordination. Ukraine primarily served as a recipient of post-incident support during its initial interactions with foreign cybersecurity assistance. However, since 2022, it has taken on a more active and integrated role in global cyber defence frameworks. Instead of receiving aid in isolation, Ukraine now actively collaborates with its partners to develop and implement its defence strategies. Real-time diagnostics and operational feedback during live incidents have been made possible by organisations like the CCDCOE and NATO's VCISC. First used in times of conflict, the EU's Cyber Rapid Response Teams involved Ukrainian teams in peer-to-peer cooperation rather than hierarchical guidance. Technical partnerships have become dynamic and ongoing, as evident in Ukraine's participation in ongoing dialogues, such as the EU-NATO-Ukraine Cyber Dialogue and the Structured Dialogue on Resilience. These platforms have functioned as operational centres, not just diplomatic forums.

[373] Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). CYBERSECURITY: LEGAL AND ORGANIZATIONAL SUPPORT IN LEADING COUNTRIES, NATO AND EU STANDARDS. *Journal of Security & Sustainability Issues*, *9*(3).

The third and most strategic shift is the movement from symbolic alignment with Euro-Atlantic norms to operational integration into them[374]. Ukraine's cybersecurity architecture is increasingly based on the norms, procedures, and legal frameworks of both NATO and the EU, despite the country's formal exclusion from both organisations. This entails the technical adoption of secure-by-design architectures throughout the energy industry, the implementation of cyber crisis management protocols developed through PESCO, and legal harmonisation with the NIS2 Directive. Ukraine has also begun contributing to initiatives that look to the future, such as the NATO Innovation Fund and DIANA. Its contributions now extend beyond compliance to include knowledge production, providing insights from the battlefield that actively influence future cybersecurity policy in the Euro-Atlantic region.

Together, these three developments confirm that Ukraine's response to cyber threats has been profoundly reshaped by its engagement with NATO and EU structures. What started as a necessity-driven reactive system has developed into a proactive, integrated, and strategically aligned defence posture. This change responds to the thesis's research puzzle proving that Ukraine has experienced an impact in protecting itself from Russian cyberattacks on its vital infrastructure as a result of its integration into Euro-Atlantic cybersecurity frameworks.

Institutionalized Support and Measurable Change

As already noted in sections 3.1.2 and 3.2.1, Ukraine's cyber development was not accomplished in isolation. Still, it was enabled by an intensified framework of Euro-Atlantic support mechanisms, which became consolidated, and integrated into Ukraine's national administrative system.

Prior to 2022, Ukraine's engagement with EU and NATO cybersecurity frameworks remained largely preparatory in nature, focusing on policy harmonisation, joint training, and strategic coordination. However, the post-invasion period was marked by a clear shift to operational domain activities. Trainings such as Locked Shields and Crossed Swords, with which Ukraine's CERTs were familiar, evolved from simulations to being real-time model benchmarks for crisis management in cyberspace. By actively collaborating with foreign partners, Ukraine has significantly enhanced its domestic incident response capabilities. The full-scale invasion

[374] Bond, I., & Scazzieri, L. (2022). *The EU, NATO and European security in a time of war*. Brussels: Centre for European Reform.

hindered the physical deployment of the EU's Cyber Rapid Response Teams (CRRTs), which were activated in February 2022 to support Ukraine. However, the partnership made it easier for Ukraine to incorporate best practices and tools into its cybersecurity framework. In a similar vein, Ukraine has been able to perform real-time triage, containment, and forensic analysis during cyber incidents thanks to remote assistance from NATO's Virtual Cyber Incident Support Capability (VCISC).

Additionally, activities aimed at legal and strategic convergence, exemplified by ENISA's technical guidelines on the application of the NIS2 Directive and the establishment of EUAM cyber advisers, progressed from purely advisory roles toward direct institutional empowerment. These activities did not reflect traditional best practice but enabled an active defence posture. The ability of Ukraine to detect lateral movements in the October 2022 attack and to mitigate the impact of logic bomb attacks, such as Industroyer2, is an example of this evolution.

What defines the resilience stage after 2022 is not merely the availability of support from the EU and NATO, but Ukraine's capacity to absorb and apply that support in a timely fashion. The real change is reflected in Ukraine's shift from being a mere recipient of expertise to becoming an active participant and partner in shaping common cyber defence standards and procedures. This provides strong indications for my hypothesis that the harmonisation of NATO and EU cybersecurity policy has played a significant role in strengthening Ukraine’s resilience and capacity.

Internal Reforms and Cultural Change

Ukraine has taken significant internal measures to enhance the resilience of its energy infrastructure, in addition to receiving allied support from the European Union and NATO. These include updating the industrial control system, developing standard network monitoring protocols, and developing incident response plans specifically designed to address threats to vital infrastructure. Ukraine was able to improve its responsiveness and anticipate and prevent cascading effects in possible future incidents by implementing these Euro-Atlantic standard-based changes.

The development of a cybersecurity-aware culture, especially among operational staff in the energy sector, was arguably the most significant internal shift. In contrast to the ad hoc

awareness of 2015, employees in the energy sector received regular training in cyber hygiene and threat recognition by 2024[375]. Ukraine's general legal and policy harmonisation with EU models has made it possible for this change to occur not just in terms of technical adaptation but also in terms of cultural development. However, there are still weaknesses, particularly in older municipal systems. Older protocols, such as Modbus TCP, are still vulnerable to disruption, as demonstrated by the FrostyGoop attack. Ukraine's alignment with EU digital infrastructure initiatives actively promotes the need for both continuous modernisation and adoption of industry-standard practices, despite the significant progress made by Ukraine's national systems.

Evaluation: Measuring Impact Over Time

The ten-year trajectory from the 2015 blackout to FrostyGoop's mitigation in 2024 demonstrates the resilience of nations and the effectiveness of international collaboration in the face of adversity.

The ability to comprehend attacks, assess their effects, and adjust in ways that gradually fortify the system over time is what defines true cybersecurity success, rather than the complete avoidance of all breaches. A steady trajectory of resilience is evident in the pattern that emerges from nearly ten years of cyber operations against Ukraine. However, the primary analytical query still stands: *has the integration of NATO and EU cybersecurity frameworks tangibly reduced the severity and impact of cyberattacks on Ukraine's critical infrastructure?*

Examining the technical nature of the attacks before and after 2022 as well as the results, taking into account the amount of damage caused, the speed at which Ukraine responded, and whether or not any disruption was prevented or minimised, will help determine how Ukraine's growing cybersecurity cooperation with the European Union and NATO has affected reducing the adverse effects of cyberattacks on critical infrastructure.

Prior to 2022, cyberattacks had a severe and obvious impact on Ukraine's energy sector. Blackouts were the outcome of the two most well-known incidents. More than 230,000 customers experienced several hours of power outages in three regions in 2015. When a vital transmission substation was taken out of service in 2016, the attackers attempted to compromise

[375] Streltsov, L. (2017). The system of cybersecurity in ukraine: principles, actors, challenges, accomplishments. *European Journal for Security Research*, *2*(2), 147-184.

the protective relays to cause extensive damage to the equipment. Ukraine was unprepared in each case.

Reactivity and manual intervention were hallmarks of the response, requiring engineers to physically visit substations to restore power. Power was restored due to a lack of centralised coordination, forensic capabilities, and established national protocols, but operations and mental health suffered greatly as a result. Legislative alignment with NATO or EU cybersecurity standards in Ukraine at that time was limited, and there was high reliance on foreign technical assistance following the successful execution of the attacks.

On the other hand Ukraine had to deal with increasingly sophisticated and complex cyberattacks, after 2022 it showed a consistent ability to identify, mitigate, or handle threats more quickly and with much less long-term impact[376]. A perfect example is the April 2022 Industroyer2 attack, which was successfully stopped before any damage was done because of advancements in monitoring, international collaboration, and prompt incident response.

Even in the October 2022 attack, which resulted in a blackout, the impact was more localised and transient, and Ukrainian agencies, along with NATO and EU-friendly cyber defence stakeholders, investigated and responded promptly. The 2024 Lviv attack disrupted city heating for two days but was contained swiftly, with minimal damage and quick restoration of services, despite introducing new malware and targeting smaller-scale infrastructure.

This is an evident change in the result. Ukraine has not been capable of warding off each assault, however, the impacts of these assaults, quantified regarding extent, duration, and degradation of networks, have lessened significantly. This cannot exclusively be credited to advancements in technology[377].

The adoption of crisis management structures based on NATO doctrines, Ukraine's involvement in NATO cyber defence exercises, its integration into the European Union's Cyber Rapid Response Team network, and its harmonisation with legal frameworks such as the NIS2 Directive all represent a more comprehensive systemic shift. NATO–EU collaboration appears to have contributed to reducing the severity and persistence of cyberattack impacts. This demonstrates how Ukraine has transitioned toward quicker response and more proactive defence strategies in key sectors such as energy, though some legacy vulnerabilities remain. This

[376] Lewis, J. A. (2022). *Cyber war and Ukraine*. Center for Strategic and International Studies (CSIS).
[377] *Ibidem.*

evidence supports the hypothesis while also highlighting the complexity of attributing causality in cyber resilience.

Over time, the impact of cyberattacks has been increasingly mitigated, though not entirely deterred. This comparative analysis demonstrates the strategic significance of Ukraine's cyber alignment with its Euro-Atlantic allies inferring that, once formally established, can lead to relative reduction in the scope and duration of adverse impacts[378].

The takeaway from this experience is that a war zone can be transformed into a testing ground for collective defence ideas and a target into a partner when meaningful integration into Euro-Atlantic institutions is based on substantive engagement rather than nominal alignment. When combined, this comparative study and the supporting data in this section answer the thesis's hypothesis by showing how Ukraine's strategic alignment with the NATO and EU cybersecurity frameworks has impacted its cyber resilience and its defences against cyberattacks.

3.3.1. The Importance of Mitigating Cyberattacks

In addition to being a critical national issue, mitigating cyberattacks on Ukraine's critical infrastructure, such as the energy sector, is also a shared strategic challenge for NATO and the European Union. Ukraine, which is situated on Europe's eastern border, serves as a vital buffer state between the Euro-Atlantic community and Russia, its most sophisticated cyber adversary. Every successful defence against a cyberattack in Ukraine in this context not only demonstrates national resilience but also the strength and resilience of the larger European security architecture as a whole.

Cyberspace has been a crucial part of Russia's hybrid warfare that utilised Ukraine as a test site for increasingly advanced cyber tools in addition to traditional military operations to increase their effectiveness. With significant psychological and geopolitical ramifications, energy infrastructure in particular has been purposefully designed to disrupt daily life and discourage people throughout the winter[379].

---

[378] Štrucl, D. (2022). RUSSIAN AGGRESSION ON UKRAINE: CYBER OPERATIONS AND THE INFLUENCE OF CYBERSPACE ON MODERN WARFARE. *Contemporary Military Challenges/Sodobni Vojaški Izzivi*, *24*(3).

[379] Korda, D. R., & Dapaah, E. O. (2023). The Role of Cyberattacks on Modern Warfare: A Review. *International Journal of Research and Innovation in Applied Science*, *8*(7), 286-292.

Here, helping Ukraine to fight such attacks is not a charitable act but one of strategic wisdom. NATO and the EU are cognisant that cyberattacks transcend national boundaries. Deliberate or unintentional malware campaign spillover can impact networks that are interconnected across neighbouring EU and NATO member nations. Initially targeting Ukraine, the 2017 NotPetya attack ended up causing billions of dollars' worth of damage worldwide. Russia is increasingly using intelligence gathering and long-term penetration in its cyber strategies, which suggests that threats can be hidden in systems that partners and allies use[380].

The goal of the counterattack on Ukraine is to protect not only the people of Ukraine but also NATO's and the EU's digital sovereignty[381]. As a result, both organisations have made investments to strengthen Ukraine's cybersecurity framework. Due to war, the EU now views cybersecurity as a crucial element of both cognitive and operational collective resilience, rather than just an economic issue. For Ukraine, the benefits of collaboration have been tangible. With the conflict still ongoing, mitigation has shifted from a reactive to a proactive mode. Ukraine now anticipates attacks, detects and neutralises threats more quickly, and resumes operations with minimal disruption.

Furthermore, Ukraine's cyber maturity has become a two-way value proposition. Ukraine is increasingly offering battle-tested insight into the development of Euro-Atlantic cyber doctrine. It is not merely being defended, it is helping redefine what cyber defence is in wartime settings.

Mitigation measures possess not only practical dimensions but also significant symbolic and social implications. The establishment of effective cybersecurity in Ukraine functions as a form of cognitive defence; it serves to sustain public morale, counteract disinformation, and exemplifies the possibility of resilience even in the face of siege. These actions have consequential effects on European populations observing the unfolding conflict, as they bolster trust in the European Union's capacity to safeguard its democratic allies while simultaneously challenging the prevailing narrative of inevitable vulnerability.

To put it briefly, helping Ukraine counter cyberattacks goes beyond pure defence. It is about creating a strong, interoperable, and forward-looking European cyber framework. It is also about protecting critical infrastructure, not just in Kyiv or Lviv, but also in Tallinn, Warsaw, and Berlin.

---

[380]Kelemen, R. (2023). *Connections: The Quarterly Journal Partnership for Peace Consortium of Defense Academies and Security Studies Institutes Creative Commons BY-NC-SA 4.0 The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations*.

[381] Bonin, A. (2025). The Impact of the Ukraine War on European Cybersecurity Policies and Legislation for Critical Infrastructure, Including Energy. In *The Palgrave Handbook of Cybersecurity, Technologies and Energy Transitions* (pp. 1-40). Cham: Springer Nature Switzerland.

It is about upholding the principle that no country confronted with the realities of hybrid warfare should face them alone.

3.3.2. Further Cyber Advancements

Kyiv has strengthened its digital resilience by enacting significant reforms in response to the growing threat landscape. To formalise risk management throughout the government and vital infrastructure, Ukraine has implemented the updated NIST Cybersecurity Framework 2.0 domestically. This action is a significant step towards formalising cyber resilience best practices[382]. At the same time, Ukraine increased the operational use of its Delta situational awareness system, which supports military and cyber operations by combining intelligence, drone, and satellite data. The Brave1 technology cluster, which included AI and cyber-focused solutions, complemented these internal contributions and sped up the development of defence technology.

NATO and the EU strengthened their strategic cyber cooperation with Ukraine on a global scale[383]. Through its Comprehensive Assistance Package (CAP), which included non-lethal aid and the development of cyber defence capabilities, NATO continued to support the nation. An example to consider is the Tallinn Mechanism, which was introduced in late 2023 and raised more than €200 million to improve Ukraine's cyber infrastructure while coordinating civilian cyber assistance[384]. Additionally, the European Union used both operational and regulatory tools to advance its cyber policy. In 2024, NATO and the EU held their first Structured Dialogue on Cyber, an institutional platform which will assist in enabling a joint response to shared threats, as well as set the stage for future collective action.

In the future, bilateral as well as multilateral plans are being written to sustain and further enhance this cooperation. The EU's "Readiness 2030" strategy seeks to reduce reliance on third-country defence vendors and includes a €150 billion loan facility, with cyber defence one of the principal areas for investment[385]. At the same time, NATO and EU members are exploring

[382] Gushchyn, O., Kotliarenko, O., Panchenko, I., & Rezvorovych, K. (2022). Cyber Legislation in Ukraine: Current Status and Development Prospects. *Futurity Economics&Law*, *2*(1), 4-19.
[383] Mohd, B., & Abbas, S. (2022). Globalisation and the Changing Concept of NATO: Role of NATO in Russia-Ukraine Crisis. *Issue 5 Int'l JL Mgmt. & Human.*, *5*, 683.
[384]NATO (2024). *Comprehensive Assistance Package (CAP) for Ukraine*. [online] NATO.
[385]Munson, C., Keaton, B., Do, L., Monahan, J., Baylor, J., Tanaka, C., & O'Keefe, R. (2020). European Defense: Strategic Choices for 2030.

the development of integrated cybersecurity centres in a bid to enhance information exchange, coordinate threat intelligence, and improve rapid reaction capabilities.

Taken as a whole, these initiatives demonstrate the shift from reactive to more proactive, cooperative, and sustained cybersecurity efforts. As much as its national resilience is being enhanced, Ukraine's integration into NATO and EU cyber infrastructures is a strategic component of the wider Euro-Atlantic digital security network.

3.3.3. Remaining Gaps and Challenges

In spite of the strides by Ukraine in developing its cybersecurity through aligning with the EU and NATO, there are many weaknesses that still exist, highlighting both the depth of improvement and the remaining gaps that require attention.

Due in large part to structural reforms, harmonised legislation, enhanced training, and Euro-Atlantic integration of cyber norms, Ukraine's energy sector has significantly improved its resilience since the initial cyberattacks in 2015 and 2016. However, as the war progressed and the threats changed, it became clear that even though international assistance is crucial, it cannot protect every front or replace long-term, systemic change[386].

The ongoing vulnerability of municipal and decentralised infrastructure, particularly in those sectors that still rely on legacy technologies, is one of the most significant flaws that continues to affect Ukraine's cyber resilience. Older protocols, such as Modbus TCP, are still widely used and often lack even the most basic security features, as demonstrated by the FrostyGoop attack on Lviv's heating grid in 2024. Cloud migration, cooperative training exercises, and EU-funded modernisations have helped the national grid, but smaller energy providers usually lack the technical know-how and resources to successfully implement such measures[387]. These regional systems continue to be soft targets, indicating a discrepancy in sector-wide standardisation that EU digital infrastructure projects aim to address but have not yet eliminated.

Furthermore, although Ukraine has benefited from institutional adaptation, this adaptation is still relatively new and uneven. Many of the operational doctrines, cyber policies, and crisis response

[386] Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European union and nato global cybersecurity challenges. *Prism*, *6*(2), 126-141.

[387] Davydiuk, A., & Zubok, V. (2023, May). 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)* (pp. 121-139). IEEE.

frameworks that currently govern Ukraine have been created under pressure, in a state of war[388]. The long-term viability of these structures will require sustained investments in workforce development and intersectoral implementation, in addition to infrastructure and legislation. These gains, though genuine, are still predicated on an ad hoc framework of internal and external support, as recent studies have shown, and they have not yet attained the degree of institutionalisation observed in more stable, peacetime regimes.

An additional source of risk is also introduced by Ukraine's reliance on ad hoc agreements with private sector companies, particularly in the fields of technical threat analysis and cloud computing[389]. For example, while the quick transfer of data to Western cloud services protected important assets from possible loss, this approach relies on goodwill and access to foreign technology. Furthermore, it opens up new attack vectors because, despite their relative security, cloud environments do require some safeguards, and security experts need to quickly adapt to the complexity of hybrid networks[390]. These arrangements remain intrinsically vulnerable and may prove unreliable during prolonged periods of crisis in the absence of a mature, sovereign cloud infrastructure or a unified public-private cybersecurity strategy.

In a broader sense, Ukraine's experience has revealed a structural conflict in the way the EU and NATO support mechanisms are coordinated. Strategic alignment is still hampered by fragmented governance, a lack of a single command, and divergent operational doctrines, despite the significant contributions made by both institutions through tools such as the CRRTs, VCISC, and legal approximation with NIS2[391]. In particular, the EU-NATO paradigm falls short in addressing issues such as collective cyberattack attribution, private company participation in cyber response plans, and coordinating offensive and defensive policies. As the war in Ukraine brutally demonstrated, these deficiencies are by no means unique to Ukraine but rather represent a more widespread lack of coordination in European cyber policy.

Lastly, while rapid response capacity has been dramatically improved, multilateral structures for long-term collective action, such as enduring threat intelligence sharing, cyber diplomacy

---

[388] Strukova, S., Albaladejo-González, M., Bozhilova, M., Fuentes, A. C., Lenti, S., Perez, G. M., ... & Ruipérez-Valiente, J. A. (2024, May). Bridging the Gap: Cyber Defence Skills for the Future. In *2024 IEEE Global Engineering Education Conference (EDUCON)* (pp. 01-10). IEEE.

[389] Rattray, G., Brown, G., & Moore, R. T. (2023). The Cyber Defense Assistance Imperative: Lessons from Ukraine. *Aspen Institute*, *14*.

[390] *Ibidem.*

[391] 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. *Policy Department for External Relations Directorate General for External Policies of the Union. https://www. europarl. europa. eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI (2023) 702594_EN. pdf*.

coordination, and cloud defence interoperability, remain underdeveloped[392]. Ukraine's defensive success, while impressive, is not fully replicable without continuous strategic investment by its allies. The challenge is not so much withstanding the next attack, but building a system that can prevent, recover, adapt, and absorb on its own, something that requires more investment, training, and long-term thinking.

Ukraine has mostly overcome the challenge of aligning its cybersecurity architecture with NATO and EU standards, despite a few inconsistencies. Institutional coordination between different levels has undoubtedly improved over the years. Despite this, the country still suffers from massive cyber attacks, especially during the period of armed conflict[393]. This thus raises the question, how much of these changes have made a practical difference, is actually on the ground.

On a less optimistic note, it is fair to observe that integration within Euro-Atlantic institutions could be a double-edged sword. It had certainly lent a helping hand to Ukraine's modernisation in cyber terms and on the other could have possibly opened up the country to the West, i.e., Russia which had a hidden agenda[394]. This sort of strategic vulnerability could be the rationale for why Ukraine has been attacked, successfully rendering the nation that sits at the epicentre of the geopolitically motivated undercurrent tensions.

This kind of cyber assistance should then be more than neutral and apolitical. It goes beyond highly political action, as measures that extend beyond the realm of cybersecurity[395]. As western partners of Ukraine step up efforts to cooperate with Ukraine, it is equally essential to realise the implications of such actions. Any future strategy aimed at making Ukraine more resilient will need to factor in the unpredictability of solutions to the issue[396].

In conclusion, it is undeniable that Ukraine's collaboration with the EU and NATO has raised the bar for cyber resilience. Ukraine's current cybersecurity posture is significantly more extensive, swift, and professional than it was prior to 2022. Long-standing weaknesses, particularly in cloud migration policy, private-sector reliance, municipal infrastructure, and alliance coordination, indicate that the task is far from being completed. These limitations underscore a

---

[392] *Ibidem.*

[393] Kostyuk, N. and Brantly, A. (2022) 'War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation', *Contemporary Security Policy*, 43(3), pp. 498–515.

[394] *Ibidem.*

[395] *Ibidem.*

[396] 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. *Policy Department for External Relations Directorate General for External Policies of the Union. https://www. europarl. europa. eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI (2023) 702594_EN. pdf.*

central idea of this thesis: although international assistance can be transformative, it must adapt to keep pace with the evolving threat. NATO and the EU must not only maintain their current levels of engagement but also intensify their efforts to enable Ukraine to sustain and build upon its gains. This includes bridging existing gaps, simplifying support systems, and funding long-term, interoperable solutions that extend beyond crisis management to create systemic, future-proof resilience.

This thesis recognises that the evolving nature of cyber conflict and the absence of fully transparent data on classified cyber operations limit the scope of conclusive assessments. As such, interpretations of resilience and effectiveness are based primarily on publicly available strategies and reported incidents.

CONCLUSIONS

The path traced in this thesis unfolded along three fundamental axes: the definition and evolution of cyberspace as a new domain of conflict; the normative and strategic response of the main Western alliances, NATO and the European Union, to this transformation; and finally, the concrete and dynamic analysis of the Ukrainian case as a testing ground for the new architectures of cyber defence. Each chapter has contributed, from different but complementary perspectives, to building a broader framework that today proves essential for understanding contemporary hybrid warfare and the structural vulnerabilities that global digitalization has exposed, and in many cases, amplified.

Chapter I, addressed the ontological and strategic question of cyberspace: from an abstract concept to a core infrastructure of the modern world, from a space of communication to an operational theatre of war. We have seen how the progressive militarization of digital space has turned cyberspace into a true "fifth domain," where the classical logics of conflict recombine with the possibilities offered by anonymity, instantaneity, and the transversality of code. Far from being a neutral space, cyberspace emerges as a critical mirror of political tensions, power asymmetries, and systemic fragilities that define the contemporary international order. The analysis of actors, tools, and operational logic has shown how the lines between peace and war, civil and military, defence and surveillance, are today deeply blurred and unstable.

Chapter II, shifted the focus to the institutional and normative mechanisms developed to respond to the growing cyber threat. The European Union and NATO emerge as key players in the attempt to build a shared governance of digital security. The NIS and NIS2 directives, joint strategies, coordination agencies, and crisis simulations represent the tools being used to counter a threat that, by nature, escapes the traditional boundaries of international law and territorial sovereignty. However, the analysis has also revealed how these architectures, despite becoming increasingly sophisticated, are still marked by structural asymmetries, unequal resources, and cultural divergences among member states. The push for harmonization clashes with a reality made of sovereign resistance, industrial competition, and a limited culture of shared risk. Moreover, there is a tangible risk that cybersecurity is being approached as a purely technical matter, ignoring its deeply political nature, tied to the control of information, the management of trust, and the redefinition of sovereignty itself.

Chapter III, sought to put these hypotheses to the test by examining how the integration of Euro-Atlantic cyber defence structures has, or has not, affected the resilience of a country under attack: Ukraine. The Ukrainian case has been, and continues to be, a dramatic but revealing laboratory. The analysis of its cybersecurity architecture before and after 2022, the study of the major Russian attacks on its critical infrastructures (2015, 2016, 2022, 2024), and the comparison between its initial vulnerabilities and the countermeasures later implemented, all showed a significant evolution. Ukraine's progressive integration into NATO and EU frameworks led to a more structured policy environment, standardized practices, and improved technical capacities. Yet, the Ukrainian case also raises critical questions: How effective is this integration in the absence of full knowledge sharing? What are the costs in terms of decision-making autonomy? And how can we reconcile the logic of protection with that of deterrence, in a context where threats are constant, pervasive, and often invisible?

Ultimately, what emerges is that cybersecurity is not just a technical issue but a political, epistemological, and almost philosophical one. Defending a critical infrastructure today also means asking who controls the data, who has access to the flow of information, how trust is built among allies, and how much decision-making power a state is willing to cede in exchange for protection. In this sense, cyber defence becomes the terrain where international relations are redefined, where new forms of solidarity emerge, and where the strategic hierarchies of the 21st century are reshaped.

Cyberwar is not just a shift in instruments, it is a transformation in the purposes and meanings of conflict. It is no longer about conquering territories or resources, but about controlling systems, narratives, cognitive infrastructures. War now hides within software, protocols, invisible signals that regulate our daily lives. And for this reason, it becomes even more insidious, more pervasive, more difficult to recognize.

Cyberspace is the opaque face of our age: an intangible yet powerful web, where hopes and fears intertwine, where promises of emancipation coexist with the threat of annihilation. Writing this thesis meant looking into that reflection, restless, unstable, ambiguous, with open eyes and a watchful mind. It meant choosing not to turn away from these new, silent forms of power.

In a world where borders are drawn with strings of code and attacks make no noise but shatter balances, defence can no longer be merely reactive: it must be vision, it must be culture, it must be awareness. Real resilience lies not only in firewalls or specialized agencies, but in the

collective ability to understand, anticipate, and transform.

And so Ukraine has transformed from a target into a symbol—not only of resistance, but of regeneration. At the heart of the crisis, it has built new networks, not only digital, but also human, political, and strategic.

This thesis does not solve a problem, it opens a question. A question that concerns each of us: How far are we willing to go to defend what we cannot see, but on which we entirely depend?

And if it is true that every network carries its own knots, then it is precisely there, in the cracks that we must learn to look. Not with fear, but with clarity. Because it is within those invisible folds that the future of our security is being shaped. And perhaps, our freedom too.

BIBLIOGRAPHY

Agbeleye, O. (2022). *What Is Cybersecurity? A Complete Overview Guide*. [online] Springboard Blog. Available at: https://www.springboard.com/blog/cybersecurity/what-is-cybersecurity/.

Allianz Commercial. (2024). *Allianz Risk Barometer 2024 - Cyber incidents*. [online] Available at: https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2024-cyber-incidents.html.

Allyn, B. (2022). Deepfake Video of Zelenskyy Could Be 'Tip of the Iceberg' in Info war, Experts Warn. *NPR*. [online] 16 Mar. Available at: https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

Anagnostakis, D. (2025). "Taming the Storm" of Hybridity: The EU-NATO Relationship on Countering Hybrid Threats – From Functional Overlap to Functional Cooperation. *Defence Studies*, 1-25.

Andrii Bezverkhyi (2022). *Detect Mars Stealer Cryptojacking Malware*. [online] SOC Prime. Available at: https://socprime.com/blog/detect-mars-stealer-cryptojacking-malware/.

Antoniuk, D. (2025). *Ukrainian cyber market grows amid war but still lacks support and funding, report says*. [online] Therecord.media. Available at: https://therecord.media/ukraine-cybersecurity-market-study-datadriven.

Arquilla J. & Ronfeldt D. (1993). Cyberwar is coming! Santa Monica, CA: RAND Corporation

Axon, L., Saunders, J., Esteve-González, P., Carver, J., Dutton, W., Goldsmith, M., & Creese, S. (2025). Private-public initiatives for cybersecurity: the case of Ukraine. *Journal of Cyber Policy*, 1–24.

Bagwe, M. (2025). *Ukraine Experiences Internet Outage - and Russia May, Too*. [online] Cio.inc. Available at: https://www.cio.inc/ukraine-experiences-internet-outage-russia-may-too-a-18806.

Barlow, J.P. (1996). *A Declaration of the Independence of Cyberspace*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/cyberspace-independence.

Barlow's, J. P. (1990). Crime and Puzzlement.

Barth T. H. (2024) Cyberspace and Space Similarities, Differences, and Related National Security Issues. Institute for Defence Analyses.

BAY, T. (2022). *KnowBe4 Report Reveals Critical Infrastructure Under Siege with Cyber Attacks Increasing 30 Percent in One Year*. [online] Knowbe4.com. Available at: https://www.knowbe4.com/press/knowbe4-report-reveals-critical-infrastructure-under-siege-with-cyber-attacks-increasing-30-percent-in-one-year.

BLACKSEA CASPIA. (2024). *The Sectors Most Targeted by Cybercrime*. [online] Available at: https://blacksea-caspia.eu/en/sectors-most-targeted-cybercrime

Blumfelde S.(2022). The role of international organisations in global cybersecurity governance.

Bond, I. and Scazzieri, L. (2022). *The EU, NATO and European security in a time of war*. [online] Centre for European Reform. Available at: https://www.cer.eu/publications/archive/policy-brief/2022/eu-nato-and-european-security-time-war.

Bondarenko, I.D., Shestakov, V.I., 2023. RUSSIAN CYBERATTACKS ON UKRAINE – A WAR CRIME. Juridical scientific and electronic journal 614–619. doi:10.32782/2524-0374/2023-11/152

Bonin, A. (2025). The Impact of the Ukraine War on European Cybersecurity Policies and Legislation for Critical Infrastructure, Including Energy. In *The Palgrave Handbook of Cybersecurity, Technologies and Energy Transitions* (pp. 1-40). Cham: Springer Nature Switzerland.

Borghard, E. D. and Lonergan, S. W. (2021) Deterrence by denial in cyberspace, *Journal of Strategic Studies*, 46(3), pp. 534–569. doi: 10.1080/01402390.2021.1944856.

Borychenko, O.et al.. (2024). CYBERSECURITY IN THE ENERGY INDUSTRY OF UKRAINE: PROTECTION MEASURES AND CHALLENGES IN THE CONTEXT OF ENERGY SECURITY. *Revista Gestão & Tecnologia*, *24*(4), 67-90

Boyte, K.J., (2020). A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare, in: Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications. IGI Global, pp. 1214–1231. doi:10.4018/978-1-7998-2466-4.ch071

Brachiella A. (2022). Policy paper number 281. Cyberattacks In Russia's hybrid war against Ukraine, and its ramifications for Europe. Notre Europe, Jacques Delors Institute.

Brantly, A. (2022). Battling the bear. *Cyber Security Politics*, [online] pp.157–171.

Brocardi.it. (2023). *Servizi pubblici essenziali - Dizionario Giuridico*. [online] Available at: https://www.brocardi.it/dizionario/193.html

Bronk, C., Collins, G. and Wallach, D. (2023). *FALL 2023 | 33 The Ukrainian Information and Cyber War*. [online] Available at: https://cyberdefensereview.army.mil/Portals/6/Documents/2023_Fall/CDR_V8N3_Fall_2023_03-Bronk.pdf?ver=U0B1Cl6qzBlZrFPxIjqOEg%3d%3d.

Burton, J. (2015) NATO's cyber defence: Strategic challenges and institutional adaptation. Defence Studies. 15 (4), 297-319.

Business, C.D., CNN (2020). *Cyber attacks are increasingly all about financial gain, report says*. [online] CNN. Available at: https://edition.cnn.com/2020/05/19/tech/data-breach-report-verizon/index.html.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*, *31*(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Campanale, G. (2025). *ContentKeeper Content Filtering*. [online] Cybersecurity360.it. Available at: https://www.cybersecurity360.it/nuove-minacce/dal-concetto-di-cyber-attack-al-cyberwarfare-luso-della-forza-in-ambito-cyber/

Cenetti C. (2014), Cybersecurity: Unione Europea e Italia. Prospettive a confronto, p. 25.

Cerf, E. (2024). *Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world*. [online] News. Available at: https://news.ucsc.edu/2024/05/ukraine-cybersecurity/.

Ceuca, R. (2024). *The IT Army of Ukraine's Cyber Operations against Russian Wartime Assets NOTHING QUIET ON THE EASTERN DIGITAL FRONT*. [online] Available at: https://newstrategycenter.ro/wp-content/uploads/2024/06/NOTHING-QUIET-ON-THE-EASTERN-DIGITAL-FRONT_NSC.pdf.

Choucri, N. (2013). Cyberpolitics in international relations. *Choice Reviews Online*, 50(12), pp.50–699350–6993. doi:https://doi.org/10.5860/choice.50-6993.

CISA (2021). *Cyber-Attack Against Ukrainian Critical Infrastructure*. [online] Cybersecurity and Infrastructure Security Agency.

CISA (2024). *Russian Military Cyber Actors Target US and Global Critical Infrastructure | CISA*. [online] Cybersecurity and Infrastructure Security Agency CISA. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a.

Clarke, R. A., & Knake, R. K. (2014). Cyber war. Old Saybrook: Tantor Media, Incorporated.

Cloudflare (2024). Shielding the Future: Europe's Cyber Threat Landscape Report.

Collinson M. -Monahan B. - Pym D. (2012). A Discipline of Mathematical Systems Modelling. London: College Publications.

Comitato Atlantico Italiano (2025). *Quale approccio per una minaccia nuova? - Comitato Atlantico Italiano*. [online] Comitato Atlantico Italiano. Available at: https://www.comitatoatlantico.it/studi/quale-approccio-per-una-minaccia-nuova/ .

Consilium. (2024). *EU-NATO cooperation*. [online] Available at: https://www.consilium.europa.eu/en/policies/eu-nato-cooperation/.

Copeland, B.J. (2024). Artificial intelligence. In: *Encyclopedia Britannica*. [online] Available at: https://www.britannica.com/technology/artificial-intelligence.

Costigan , S.S. and Hennessy, M.A. (2024). *HYBRID THREATS AND HYBRID WARFARE REFERENCE CURRICULUM*. [online] *NATO Headquarters Brussels*.

Council of Europe (2024). *CyberEast+ Activities*. [online] Cybercrime.

Council of the EU (2022). *Ukraine: Declaration by the High Representative on behalf of the European Union on the cyberattack against Ukraine*. [online] www.consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

Cristiano F. (2023). The Blurring Politics of Cyber Conflict: A Critical Study of the Digital in Palestine and Beyond. Lund University.

CYBER DIIA (2024). *A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience A comprehensive review*. [online] Available at: https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf.

Cybersecurity and Infrastructure Security Agency (CISA). Known Exploited Vulnerabilities Catalog.

Cybersecurity Guide Contributors (2025). *Cybersecurity and environmental services and infrastructure*. [online] Cybersecurity Guide. Available at: https://cybersecurityguide.org/industries/environmental-protection/.

DAI Global, LLC (2021). *USAID CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE REVIEW OF THE REGULATORY FRAMEWORK FOR CRITICAL INFRASTRUCTURE CYBERSECURITY IN UKRAINE: LEGISLATIVE ASSESSMENT REPORT*.

Dareen, S. and Vallari, S. (2024). *Cyberattacks on US utilities surged 70% this year, says Check Point*. [online] Reuters. Available at: https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/.

Davydiuk, A., & Zubok, V. (2023, May). 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)* (pp. 121-139). IEEE.

Defence Industry Europe (2024). *Council of the European Union approves PESCO Strategic Review*. [online] Defence Industry Europe. Available at: https://defence-industry.eu/council-of-the-european-union-approves-pesco-strategic-review-to-strengthen-defence-integration/.

Department of Homeland Security (2010) 'IT Program Assessment: NPPD – Critical Infrastructure Warning Information Network (CWIN).

Desetty, A., Reddy Pulyala, S. and Dutt, V. (2023). Protecting Critical Infrastructure from Cyber Attacks: A Multifaceted Approach. *International Journal For Advanced Research in Science and Technology*, [online] 13(8). Available at: https://ijarst.in/public/uploads/paper/622751701751637.pdf .

Digital Watch Observatory. (2024). *Cybersecurity Strategy of Ukraine | Digital Watch Observatory*. [online] Available at: https://dig.watch/resource/cybersecurity-strategy-of-ukraine.

Digmelashvili, Temur (2023) The Impact of Cyberwarfare on the National Security. *Future Human Image*, Volume 19, 12-19. https://doi.org/10.29202/fhi/19/2

Don, J. (2017). *Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack*. [online] blog.isa.org. Available at: https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware.

Douglas O. (2024) On Cyber War. The Cove.

Dragos, Inc. (2023). ICS/OT Cybersecurity Year in Review.

Drent, M., Dinnissen, R., Van Ginkel, B., Hogeboom, H., Homan, K., Zandee, D., Rood, J. and Meijnders, M. (2014). *The relationship between external and internal security Clingendael Strategic Monitor Project*. [online] Available at: https://www.clingendael.org/sites/default/files/pdfs/The%20relationship%20between%20external%20and%20internal%20security.pdf.

Duguin, S. and Pavlova, P. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. [online] European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.

Dunn Cavelty M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge.

Eda.europa.eu. (2022). *Activation of first capability developed under PESCO points to strength of cooperation in cyber defence*. [online] Available at: https://eda.europa.eu/news-and-events/news/2022/02/24/-of-first-capability-developed-under-pesco-points-to-strength-of-cooperation-in-cyber-defence.

EEAS Press Team (2022). *Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue | EEAS Website*. [online] www.eeas.europa.eu. Available at: https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en.

Eichensehr, K.E., (2022). Ukraine, Cyberattacks, and the Lessons for International Law, in: AJIL Unbound. Cambridge University Press, pp. 145–149. doi:10.1017/aju.2022.20

ENISA (2016).ENISA's Position on the NIS Directive. Version 1.0.

ENISA (2019). *What we do | ENISA*. [online] Europa.eu. Available at: https://www.enisa.europa.eu/about-enisa/what-we-do.

ENISA (2024). *ENISA Threat Landscape 2024*. [online] ENISA. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

Eriksson J. - Giacomello G. (2014). International Relations, Cybersecurity, and Content Analysis: A Constructivist Approach. The Global Politics of Science and Technology - Vol. 2 (pp.205-219) Chapter 6.

EUR-Lex (2016). *Directive - 2016/1148 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng.

EUR-Lex (2017). *EUR-Lex - 52017PC0477 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN.

EUR-Lex (2019). *Regulation - 2019/881 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

EUR-Lex (2020). *Directive - 2002/19 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/dir/2002/19/oj/eng .

EUR-Lex (2020). *Directive - 2002/20 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/dir/2002/20/oj/eng .

EUR-Lex (2020). *Directive - 2002/21 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/dir/2002/21/oj/eng.

EUR-Lex (2020). *Directive - 2009/140 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/dir/2009/140/oj/eng.

EUR-Lex (2022). *Directive - 2022/2555 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

EUR-Lex (2024). *Regulation - 2024/2847 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

EUR-Lex (2025). *Communication from the Commission on a European Programme fo... - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A52006DC0786 .

EUR-Lex (2025). *Regulation - 460/2004 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/reg/2004/460/oj/eng .

EUR-Lex (2025). *Regulation - EU - 2025/38 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng .

EUR-Lex. (2022). *Directive - 2022/2557 - EN - CER - EUR-Lex*. [online] Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

EUR-Lex. (2024). *Directive - 2008/114 - EN - EUR-Lex*. [online] Available at: https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng.

EUR-Lex. (2025). *A Trusted and Cyber Secure Europe - ENISA Strategy | ENISA*. [online] Available at: https://www.enisa.europa.eu/publications/a-trusted-and-cyber-secure-europe-enisa-strategy.

European Parliament and Council (2022). *Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*. Official Journal of the European Union, L 333, 27 December 2022, pp. 164–195. Article 2 Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

European Union (n.d.). *EU support for Ukraine | European Union*. [online] european-union.europa.eu. Available at: https://european-union.europa.eu/priorities-and-actions/eu-support-ukraine_en.

European Union Agency for Cybersecurity (ENISA), 2023. *Good Practices for Supply Chain Cybersecurity*. [pdf] Available at: https://www.enisa.europa.eu/.

European Union External Action (2024). *Strengthening Cybersecurity Through Cross-Border Cooperation: Insights from Bucharest and Ivano-Frankivsk — EUAM Ukraine*. [online] EUAM Ukraine.

FBI (2018). *The Morris Worm*. [online] Federal Bureau of Investigation. Available at: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

Fick, N., Miscik, J., Segal, A. and Goldstein, G.M. (2022). *The United States Needs a New Foreign Policy for Cyberspace*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace.

Fierro, C.D. and Dwyer, J. (2022). *Caddywiper malware targeting Ukrainian organizations*. [online] Ibm.com. Available at: https://www.ibm.com/think/x-force/caddywiper-malware-targeting-ukrainian-organizations.

Fitzgerald, A. (2024). *Understanding EU Cybersecurity: History, Regulations, and Certifications*. [online] Secureframe. Available at: https://secureframe.com/blog/eu-cybersecurity.

Fleck, A. (2024). Cybercrime Expected To Skyrocket in Coming Years. [online] EBnet.

Franchina, L. and Fulgenzi, C. (2024). *Cyber Europe 2024, anche l'ACN protagonista per la resilienza dell'infrastruttura energetica - Cyber Security 360*. [online] Cyber Security 360. Available at: https://www.cybersecurity360.it/news/cyber-europe-2024-anche-lacn-protagonista-per-la-resilienza-dellinfrastruttura-energetica/.

FREE NETWORK. (2021). *Ukraine's Integration into the EU's Digital Single Market*. [online] Available at: https://freepolicybriefs.org/2021/02/15/ukraines-integration-single-market/.

Fyshchuk "Stronger together? EU support for Ukrainian local authorities facing cyber attacks (2022–2023)," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190344

Garamone, J. (2010). *Lynn notes Cyber Command's significance*. [online] Air Force. Available at: https://www.af.mil/News/Article-Display/Article/116581/lynn-notes-cyber-commands-significance.

Gibson W. (1984) Neuromancer, Ace Pub., New York.

Giordano, P. (2023). *Multi-Domain Operations in NATO - Explained - NATO's ACT*. [online] NATO's ACT. Available at: https://www.act.nato.int/article/mdo-in-nato-explained/.

Giordano, P. (2023). *NATO Centres of Excellence – Cooperative Cyber Defence (CCD COE) - NATO's ACT*. [online] NATO's ACT. Available at: https://www.act.nato.int/article/nato-centres-of-excellence-cooperative-cyber-defence-ccd-coe/.

Givens, A.D., Gorbachevsky, M., Biernat, A.C., (2023). How Putin's Cyberwar Failed in Ukraine. Journal of Strategic Security 16, 96–121. doi:10.5038/1944-0472.16.2.2099

Godwin III, J.B., Kulpin, A., Rauscher, K.F. and Yaschenko, V. (2014). *Critical Terminology Foundations 2 Russia-U.S. Bilateral on Cybersecurity*. [online] Available at: https://www.files.ethz.ch/isn/178418/terminology2.pdf .

Greenberg, A. (2024). *How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter*. [online] WIRED. Available at: https://www.wired.com/story/russia-ukraine-frostygoop-malware-heating-utility/.

Gregory, J. and Watson, I. (2024). China linked to UK cyber-attacks on voter data, Dowden to say. *www.bbc.com*. [online] 25 Mar. Available at: https://www.bbc.com/news/uk-politics-68652374.

Grossman, T. (2023). ETH Library Cyber Rapid Response Teams: Structure, Organization, and Use Cases. *Center for Security Studies (CSS), ETH Zürich*. [online]

Gushchyn, O., Kotliarenko, O., Panchenko, I., & Rezvorovych, K. (2022). Cyber Legislation in Ukraine: Current Status and Development Prospects. *Futurity Economics&Law*, *2*(1), 4-19.

Gwu.edu. (2016). *Aaron Hughes, Deputy Assistant Secretary of Defense for Cyber Policy, Office of the Secretary of Defense, 'Statement Before the House Committee on Oversight and Government Reform, Information Technology and National Security Subcommittee,' July 13, 2016. Unclassified. | National Security Archive*. [online] Available at: https://nsarchive.gwu.edu/document/21929-document-10 .

Harries, D. (2017). Narrative Mapping of Cyberspace. Context and Consequences. In J. Martín Ramírez Luis & A. García-Segura (Cur.), Cyberspace Risks and Benefits for Society, Security and Development (pp. 23-40). Berlino: Springer.

Head of the Office of the President of Ukraine A. Yermak (2024). *Cybersecurity Strategy of Ukraine | Digital Watch Observatory*. [online] Digital Watch Observatory.

Headmind Partners. (2022). *Industroyer 2 : the Russian Cyberattack on Ukraine Infrastructure*. [online] Available at: https://www.headmind.com/industroyer-2/.

Herz, J. (2003)'The security dilemma in international relations: background and present problems', International Relations 17(4), pp.411−16.

Hughes, R.B. (2009). *CustomError*. [online] csl.armywarcollege.edu. Available at: https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/NATO%20and%20Cyber%20Defence%20-%20Mission%20Accomplished.pdf.

Hyslop M. (2007). Critical Information Infrastructures. Resilience and Protection. Springer.

IDB (2021). *Cybersecurity and the Internet of Things (IoT) | IDB*. [online] Institute for Defense & Business. Available at: https://www.idb.org/cybersecurity-and-the-internet-of-things/.

Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European Union and Nato global cybersecurity challenges. *Prism*, *6*(2), 126-141.

Jackson S. (2016). NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack. The CIP Report.

Jackson-Preece, J. (2011). *Security in international relations*. [online] Available at: https://www.london.ac.uk/sites/default/files/uploads/ir3140-security-international-relations-study-guide.pdf.

Jenkinson, A., (2023). Digital Blood on Their Hands : The Ukraine Cyberwar Attacks. Digital Blood on Their Hands.

Johnson, C.S., Badger, M.L., Waltermire, D.A., Snyder, J. and Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. *Guide to Cyber Threat Information Sharing*, [online] 800-150. doi:https://doi.org/10.6028/nist.sp.800-150.

Johnson.T.A. (2015). Cybersecurity. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Webster University, St. Louis, Missouri, USA.

Johri, S. (2023). *Parasociality to the red pill, all found in Plato's cave.* [online] The Michigan Daily. Available at: https://www.michigandaily.com/arts/b-side/platos-parasocial-parable-of-the-cave/.

Kadri F. - Birregah B. & Châtelet E. (2014). "The Impact of Natural Disasters on Critical Infrastructures: A Domino Effect-based Study," Journal of Homeland Security and Emergency Management, De Gruyter, vol. 11(2), pages 217-241.

Kasper, A., Osula, A.M., Molnár, A., (2021). EU cybersecurity and cyber diplomacy1. Revista de Internet, Derecho y Politica. doi:10.7238/idp.v0i34.387469

Kaspersky Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Threat Landscape for Industrial Automation Systems: Statistics for H2 2023.

Kegley, C.W. and Raymond, G.A. (2021). *Realism in the Age of Cyber Warfare*. [online] www.ethicsandinternationalaffairs.org. Available at: https://www.ethicsandinternationalaffairs.org/online-exclusives/realism-in-the-age-of-cyber-warfare

Kelemen, R. (2023). *Connections: The Quarterly Journal Partnership for Peace Consortium of Defense Academies and Security Studies Institutes Creative Commons BY-NC-SA 4.0 The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations*.

Kolodziej Edward A. (2005) Security and International Relations. Cambridge University Press.

Korda, D. R., & Dapaah, E. O. (2023). The Role of Cyberattacks on Modern Warfare: A Review. *International Journal of Research and Innovation in Applied Science*, *8*(7), 286-292.

Kostrzewa-Zorbas, G. (2014). NATO in the new strategic environment: Cyberattacks now Covered by article 5 of the north atlantic Treaty. Studia Bezpieczeństwa Narodowego, 4(6), 397-418.

Kostyuk, N. and Brantly, A. (2022) 'War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation', *Contemporary Security Policy*, 43(3), pp. 498–515.

Kostyuk, N., & Geers, K. (2015). Ukraine: A Cyber Safe Haven?. *Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence*, 113-122.

Kovacevic A. - Nikolic D. (2015). Cyber Attacks on Critical Infrastructure: Review and Challenges. University of Belgrade.

Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*, *6*.

Krippendorff K. (2009). On Communicating, Otherness, Meaning, and Information. Fernando Bermejo (Ed.). New York, Routledge.

Kvartsiana, K. and Fellowship, R. (2023). *Ukraine's Cyber Defense: Lessons in Resilience | German Marshall Fund of the United States*. [online] www.gmfus.org. Available at: https://www.gmfus.org/news/ukraines-cyber-defense-lessons-resilience.

Lee, R. M, Assante, m. J., & Conway, T. (2018). "Analysis of the Cyber Attack on the Ukrainian Power Grid," Electricity Information Sharing and Analysis Center, pp. 1- 29, 24-25.

Lewis T.G. (2014). Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. Second Edition

Lewis, J. (2022). *Cyber War and Ukraine*. [online] www.csis.org. Available at: https://www.csis.org/analysis/cyber-war-and-ukraine.

Li, Tony Yuan. "Asymmetry in the Digital Age: Cyber Deterrence Strategies for Small States." Journal of Strategic Security 17, no. 4 (2024) : 71-88. Available at: https://digitalcommons.usf.edu/jss/vol17/iss4/5

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2016). The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE transactions on power systems*, *32*(4), 3317-3318.

Lilly, B., & Cheravitch, J. (2020, May). The past, present, and future of Russia's cyber strategy and forces. In *2020 12th International Conference on Cyber Conflict (CyCon)* (Vol. 1300, pp. 129-155). IEEE.

Linn, L. (2022). *CCDCOE*. [online] ccdcoe.org. Available at: https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/.

Lisi, S., - Gori, U. (2015). Cyber Warfare 2014: armi cibernetiche, sicurezza nazionale e difesa del business. Cyber Warfare 2014, 1-287.

Livelli, F.M.R. (2024). *Cyber security nell'era del quantum computing. Ci si difende così - Cyber Security 360*. [online] Cyber Security 360. Available at: https://www.cybersecurity360.it/outlook/cyber-security-nellera-del-quantum-computing-ci-si-difende-cosi/.

Luhn, A. (2015). *Crimea declares state of emergency after power lines attacked*. [online] the Guardian. Available at: https://www.theguardian.com/world/2015/nov/22/crimea-state-of-emergency-power-lines-attacked

Madnick, S., (2022). What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare. Harvard Business Review 1–7.

Markopoulou, D., Papakonstantinou, V., de Hert, P., (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law and Security Review 35. doi:10.1016/j.clsr.2019.06.007

Martino, L. (2018). Il Mulino -Rivisteweb. *Il Mulino*, [online] (ISSN 2240-7901). doi:https://doi.org/10.4476/89790).

Mattis, J.N. and Hoffman, F. (2005). *Future Warfare: The Rise of Hybrid Wars*. [online] U.S. Naval Institute. Available at: https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars.

Mbanaso U. - Dandaura E.S. (2015) The Cyberspace: Redefining A New World. Article published on IOSR Journal of Computer Engineering (IOSR-JCE)

McGuinness, D. (2017). How a cyber attack transformed Estonia. *BBC News*. [online] 27 Apr. Available at: https://www.bbc.com/news/39655415.

Microsoft (2024). *The foundations and new frontiers of cybersecurity A Microsoft Threat Intelligence report Microsoft Digital Defense Report 2024 Overview Overview*. [online] Available at:

https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf.

Migration and Home Affairs. (2023). *Critical infrastructure resilience at EU-level*. [online] Available at: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

Miller, C. (2016). *Inside The Ukrainian 'Hacktivist' Network Cyberbattling The Kremlin*. [online] RadioFreeEurope/RadioLiberty. Available at: https://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html.

Mohd, B., & Abbas, S. (2022). Globalisation and the Changing Concept of NATO: Role of NATO in Russia-Ukraine Crisis. *Issue 5 Int'l JL Mgmt. & Human.*, *5*, 683.

Moschetta, G. and Winslow, E. (2025). *6 things you need to know about cybersecurity in 2025*. [online] World Economic Forum. Available at: https://www.weforum.org/stories/2025/01/global-cybersecurity-outlook-complex-cyberspace-2025/

Moynihan, H. (2019). *The application of international law to state cyberattacks*. [online] Chatham House – International Affairs Think Tank. Available at: https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.

Munson, C., Keaton, B., Do, L., Monahan, J., Baylor, J., Tanaka, C., & O'Keefe, R. (2020). European Defense: Strategic Choices for 2030.

National Security and Defense Council of Ukraine. (2021). *The President of Ukraine approved a new Cybersecurity Strategy of Ukraine*. [online] Available at: https://www.rnbo.gov.ua/en/Diialnist/4976.html.

NATO (2002). *Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Cou...* [online] NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

NATO (2014). *Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO (2015). *Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/opinions_118435.htm.

NATO (2022). *A Short History of NATO*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/declassified_139339.htm.

NATO (2023). *NATO-Ukraine Commission (NUC)*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_50319.htm.

NATO (2023). *Collective Defence and Article 5*. [online] North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natohq/topics_110496.htm.

NATO (2023). *NATO and European Union launch task force on resilience of critical infrastructure*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/news_212874.htm.

NATO (2024). *Cyber defence*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO (2024). *Allies agree new NATO Integrated Cyber Defence Centre*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/news_227647.htm.

NATO (2024). *Comprehensive Assistance Package (CAP) for Ukraine*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_231639.htm.

NATO (2024). *Cyber defence*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO (2024). *Relations with Ukraine*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_37750.htm.

NATO (2024). *Relations with the European Union*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_49217.htm.

NATO (202). *What is NATO?* [online] NATO. Available at: https://www.nato.int/nato-welcome/.

NATO Cooperative Cyber Defence Centre of Excellence, 2025. *Locked Shields*. [online] Available at: https://ccdcoe.org/locked-shields/.

NATO Cooperative Cyber Defence Centre of Excellence, 2025. *The Tallinn Manual*. [online] Available at: https://ccdcoe.org/research/tallinn-manual/.

NATO Review. (2024). *NATO Review - Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure*. [online] Available at: https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html.

NATO Supreme Headquarters Allied Powers Europe (SHAPE), n.d. *Cyber Defence*. [online] Available at: https://shape.nato.int/about/aco-capabilities2/cyber-defence

Negreiro, M. (2021) *The NIS2 Directive: A high common level of cybersecurity in the EU*. European Parliamentary Research Service.

News, T.H. (2025). *CERT-UA Reports Cyberattacks Targeting Ukrainian State Systems with WRECKSTEEL Malware*. [online] The Hacker News. Available at: https://thehackernews.com/2025/04/cert-ua-reports-cyberattacks-targeting.html.

North Atlantic Treaty Organization.(2015). Fact Sheet, NATO's practical support to Ukraine. nrdc-ita.nato.int. (2024). *NATO Cyber Operation Centre*. [online] Available at: https://nrdc-ita.nato.int/operations/allied-reaction-force/nato-cyber-operation-centre.

Ohrimenco, S., Cernei, V., (2023). Cybertax: A New Approach to Cybersecuirty Risk Management. D. A. Tsenov Academy of Economics, pp. 33–37. doi:10.58861/tae.cf.cfeacmc.2023.03

Oleksii Artemchuk (2025). *Number of cyberattacks on Ukraine increased by 70% in past year*. [online] Ukrainska Pravda. Available at: https://www.pravda.com.ua/eng/news/2025/01/9/7492671/.

Owens W.A. et al. (2009). NAT'L Research Council, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 1. NRC Report

Paganini, S. (2013). *Il primo 'worm' su Internet non si scorda mai: era il 1988 e internet conobbe il 'Morris Worm' | Archeologia Informatica*. [online] Archeologia Informatica | Il primo 'worm' su Internet non si scorda mai: era il 1988 e internet conobbe il 'Morris Worm' Stefano Paganini. Available at: https://archeologiainformatica.it/2013/11/04/il-primo-worm-su-internet-non-si-scorda-mai-era-il-1988-e-internet-conobbe-il-morris-worm/ .

Pătrașcu, P. (2022) National security strategies and critical infrastructure: An analysis of the European Union member states, *Romanian Military Thinking*, 3, p. 12.

Pearson, J. (2022). Ukraine says it thwarted Russian cyberattack on electricity grid. *Reuters*. [online] 12 Apr. Available at: https://www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12/.

Pearson, J. (2023). Russian spies behind cyber attack on Ukraine power grid in 2022 - researchers. *Reuters*. [online] 9 Nov. Available at: https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/.

Pfannenstiel, M. and Cox, D. (2024). *NATO's Cyber Era (1999–2024) Implications for Multidomain Operations*. [online] Army University Press. Available at: https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/NATOs-Cyber-Era-UA/.

Pravitz S. (2021). "Das Wichtigste zum Tisax-Update". *Automobil Industrie*.

Prokip, A. (2025). *Ukraine's Energy Sector: Resilience After Three Years of Full-Scale War*. [online] Wilson Center. Available at: https://www.wilsoncenter.org/blog-post/ukraines-energy-sector-resilience-after-three-years-full-scale-war.

Proska , K. et.al. (2023). *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*. [online] Google Cloud Blog. Available at: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/.

Rattray, G., Brown, G., & Moore, R. T. (2023). The Cyber Defense Assistance Imperative: Lessons from Ukraine. *Aspen Institute*, *14*.

Reese, B. (2024). *Balanced Realism: A 21st Century Approach to International Relations Theory*. [online] Medium. Available at: https://briantreese.medium.com/balanced-realism-a-21st-century-approach-to-international-relations-theory-14bb4ba1aa0e.

Renz, B. (2019). Russian 'Hybrid Warfare': Resurgence and Politicisation. *The RUSI Journal*, *164*(3), 70–71.

Ribeiro, A. (2024). *Dragos details novel FrostyGoop ICS malware using Modbus TCP to disrupt OT operations worldwide*. [online] Industrial Cyber. Available at: https://industrialcyber.co/news/dragos-details-novel-frostygoop-ics-malware-using-modbus-tcp-to-disrupt-ot-operations-worldwide/.

Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, *157*(1), 6–13. https://doi.org/10.1080/03071847.2012.664354

Rinaldi, S. (2024). *10 years of Russian annexation of Crimea, reflections on the role of PMCs in hybrid warfare - ICoCA Blog*. [online] ICoCA Blog. Available at: https://blog.icoca.ch/10-years-of-russian-annexation-of-crimea-reflexions-on-the-role-of-pmcs-in-hybrid-warfare/.

Robles R. J. et al. Common Threats and Vulnerabilities of Critical Infrastructures. International Journal of Control and Automation.

Royal Air Force (2023). Air and Space Power Review, Vol. 18, Issue 1. Article Published on Centre for Air and Space Power Studies.

Santoro, V., Pensato, L., (2017). Critical infrastructure protection: The need for evolving standards: Mutating cyber-space and security issues in ITS, in: 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems, MT-ITS 2017 - Proceedings. Institute of Electrical and Electronics Engineers Inc., pp. 219–222. doi:10.1109/MTITS.2017.8005668

Sarkar, S., (2023). A Study on Cybersecurity Standards for Power Systems, in: Power Systems. Springer Science and Business Media Deutschland GmbH, pp. 429–450. doi:10.1007/978-3-031-20360-2_18

Schmidt, A. (2013). The Estonian cyberattacks. In Jason Healey (Cur.), The Fierce Domain – Conflicts in Cyberspace 1986-2012 (pp. 174-193). Washington, D.C.: Atlantic Council.

SCHMITT, M.N. (2013). *TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE*. [online] Available at: https://assets.cambridge.org/97811070/24434/frontmatter/9781107024434_frontmatter.pdf.

Schulze M. - Kerttunen M. (2023). Cyber Operations in Russia's War against Ukraine Uses, limitations, and lessons learned so far. Stiftung Wissenschaft und Politik German Institute for International and Security Affairs.

Scpc.gov.ua. (2024). *The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine (SCPC SSSCIP) is increasing technical capabilities of the National Center for Reserving State Information Resources.* [online] Available at: https://scpc.gov.ua/en/articles/366.

Shea, J. (2017). *How is NATO Meeting the Challenge of Cyberspace*. [online] National Defense University Press. Available at: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983740/how-is-nato-meeting-the-challenge-of-cyberspace/.

Shehod, A. (2016). Ukraine power grid cyberattack and US susceptibility: Cybersecurity implications of smart grid advancements in the US. *Cybersecurity Interdisciplinary Systems Laboratory, MIT*, *22*, 2016-22.

Shelest, H. (2023). *EU, NATO and Ukraine: Dream Team or a Triangle?* [online] Prism Ua. Available at: https://prismua.org/en/english-eu-nato-and-ukraine-dream-team-or-a-triangle/.

Shircliffe, J. E. (2010) 'THE DIGITAL BATTLEFIELD: PREPARING FOR PARITY', *The RUSI Journal*, 155(6), pp. 22–27. doi: 10.1080/03071847.2010.542665.

Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). CYBERSECURITY: LEGAL AND ORGANIZATIONAL SUPPORT IN LEADING COUNTRIES, NATO AND EU STANDARDS. *Journal of Security & Sustainability Issues*, *9*(3).

Sicurezzanazionale.gov.it. (2015). *Sistema di informazione per la sicurezza della Repubblica - a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia*. [online] Available at: https://www.sicurezzanazionale.gov.it/contenuti/i-principi-strategici-delle-politiche-di-cybersecurity .

Silva, D. (2024). *FrostyGoop the New Addition to ICS Specific Malware – Cyber*. [online] Hawaii.edu. Available at: https://westoahu.hawaii.edu/cyber/ics-cybersecurity/ics-weekly-summaries/frostygoop-the-new-addition-to-ics-specific-malware/.

Smith S. J. , Gebhard C, Graeger N., (2019), EU-NATO Relations, Running on the Fumes of Informed Deconfliction. Routledge.

Sophos (n.d.). *Threat Actors Explained: Motivations and Capabilities*. [online] SOPHOS. Available at: https://www.sophos.com/en-us/cybersecurity-explained/threat-actors.

Sopilko, I. (2024). Strengthening cybersecurity in Ukraine: Legal frameworks and technical strategies for ensuring cyberspace integrity. Legal Horizons, 21(2), 69-80.

Spînu, N. (2020). *Ukraine Cybersecurity Governance Assessment*. [online] Available at: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

State Sites of Ukraine (2025). *The history of State Cyber Protection Center*. [online] Scpc.gov.ua. Available at: https://scpc.gov.ua/en/history.

Štitilis, D., Pakutinskas, P., Malinauskaite, I., (2017). EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. Security Journal 30, 1151–1168. doi:10.1057/s41284-016-0083-9

Štrucl, D. (2022). RUSSIAN AGGRESSION ON UKRAINE: CYBER OPERATIONS AND THE INFLUENCE OF CYBERSPACE ON MODERN WARFARE. *Contemporary Military Challenges/Sodobni Vojaški Izzivi*, *24*(3).

Strukova, S., Albaladejo-González, M., Bozhilova, M., Fuentes, A. C., Lenti, S., Perez, G. M., ... & Ruipérez-Valiente, J. A. (2024, May). Bridging the Gap: Cyber Defence Skills for the Future. In *2024 IEEE Global Engineering Education Conference (EDUCON)* (pp. 01-10). IEEE.

Svintsytskyi, A.V. (2022). The system of cybersecurity bodies in Ukraine. *Revista Científica General José María Córdova*, [online] 20(38), pp.287–305. Available at: https://www.redalyc.org/journal/4762/476273700003/html/.

Swanson L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 russian-georgian cyber conflict. Loyola of Los Angeles International and Comparative Law Review, 32(2), 303-334.

Taddeo, M. (2012). *An Analysis For A Just Cyber Warfare*. [online] Available at: https://ccdcoe.org/uploads/2012/01/3_5_Taddeo_AnAnalysisForAJustCyberWarfare.pdf.

Tepper, E. (2022). *The First Space-Cyber War and the Need for New Regimes and Policies*. [online] Centre for International Governance Innovation. Available at: https://www.cigionline.org/publications/the-first-space-cyber-war-and-the-need-for-new-regimes-and-policies/ CIGI Policy Brief No. 173.

The Alan Turing Institute. (2025). *Enhancing the Cyber Resilience of Offshore Wind*. [online] Available at: https://www.turing.ac.uk/research/research-projects/enhancing-cyber-resilience-offshore-wind.

The Hacker News. (2024). *Pro-Ukrainian Hackers Strike Russian State TV on Putin's Birthday*. [online] Available at: https://thehackernews.com/2024/10/pro-ukrainian-hackers-strike-russian.html.

The Joint Research Centre: EU Science Hub. (2015). *Security of the supply chain*. [online] Available at: https://joint-research-centre.ec.europa.eu/projects-and-activities/security-supply-chain_en.

The President's National Infrastructure Advisory Council (2017). Securing Cyber Assets. Addressing Urgent Cyber Threats to Critical Infrastructure. NIAC

Tommaso De Zan, (2019). Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions. Global Cyber Security Center (5)2, 10.

Treccani. (2015). *Cyberspazio - Enciclopedia - Treccani*. [online] Available at: https://www.treccani.it/enciclopedia/cyberspazio_(Lessico-del-XXI-Secolo)/

Tsebenko, O., Ivasechko, O., Khivrenko, D., (2023). CHALLENGES AND OPPORTUNITIES FOR IMPLEMENTATION OF THE NATO CYBERSECURITY POLICY. Visnyk of the Lviv University 230–239. doi:10.30970/pps.2023.51.27

U.S. Department of Defence (2021). *DOD Dictionary of Military and Associated Terms As of November 2021*. [online] Available at: https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.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 & Sustainability Issues*, *9*(3).

Vasquez, C. (2024). *Simple 'FrostyGoop' malware responsible for turning off Ukrainians' heat in January attack*. [online] CyberScoop. Available at: https://cyberscoop.com/frostygoop-ics-malware-dragos-ukraine/.

Viganò, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of Critical Infrastructure. In International Library of Ethics, Law and Technology (pp. 157-177). (International Library of Ethics, Law and Technology; Vol. 21). Springer. https://doi.org/10.1007/978-3-030-29053-5_8

Wallander, C. (1979). See Mearsheimer 1990; and Waltz 1993. 3. See Wallander. *International Organization*, [online] 54(2), pp.705–735. Available at: https://library.fes.de/libalt/journals/swetsfulltext/9292080.pdf.

Waltz, K.N. (1979). Theory of International Politics. *International Journal*, [online] 35(3). Available at: https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20Addison-Wesley%20series%20in%20political%20science%20%20%20%201979.pdf.

Warren, M., Štitilis, D., & Laurinaitis, M. (2023). The impact of Russian cyber attackers within the Ukraine situation. *Journal of Information Warfare*, *22*(1), 88-107.

Wiener N. (1948) Cybernetics: Or Control and Communication in the Animal and the Machine, The M.I.T. Press, Cambridge, Massachusetts.

Wilcox S. (2022). *Three Pillars of Cyber Security: People – Process – Technology*. [online] Open Access Government. Available at: https://www.openaccessgovernment.org/pillars-of-cyber-security-technology/132732/.

Wortham, Anna (2012) "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?," Federal Communications Law Journal: Vol. 64: Iss. 3, Article 8. Available at: https://www.repository.law.indiana.edu/fclj/vol64/iss3/8

Xiangsui W. - Liang W. (2001). Unrestricted Warfare. China's Master Plan to Destroy America. Pan American Publishing Company, Panama

Zinchenko, O. I. (2024). Cyber terrorism: History of Ukraine and current trends. Actual Issues of Modern Science. European Scientific e-Journal, 33, 70-79. Ostrava: Tuculart Edition, European Institute for Innovation Development.

ACKNOWLEDGEMENTS

To Professor Raffaele Marchetti,

for giving me the opportunity to write this thesis and for inspiring in me, through his teaching and writings, a deep passion for International Relations. His guidance has been a continuous intellectual stimulus that I will carry with me throughout my academic and professional journey.

To my Supervisor,

I would like to express my sincere thanks to Dr. Martina Lucaccini for her constant availability, kindness, and attentiveness throughout the development of this work. Her support has been a valuable point of reference, guiding me with balance and expertise.