CYBER RESILIENCE IN UKRAINE: MEASURING RESPONCE TO CYBER THREATS IN THE CONTEXT OF HYBRID WALFARE

IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF ARTS IN INTERNATIONAL RELATIONS

BY

SOLOMIIA BESKA

SUPERVISOR: PROF. ERIN K. JENNE, PHD

DEPARTMENT OF INTERNATIONAL RELATIONS

CENTRAL EUROPEAN UNIVERSITY

VIENNA, MAY 2025

Author's declaration

I, the undersigned, **Solomiia Beska**, candidate for the MA degree of Master of Arts in International Relations declare herewith that the present thesis titled "Cyber Resilience in Ukraine: Measuring Response to Cyber Threats in the Context of Hybrid Warfare" is exclusively my own work, based on my research and only such external information as properly credited in notes and bibliography.

I declare that no unidentified and illegitimate use was made of the work of others, and no part of the thesis infringes on any person's or institution's copyright.

I also declare that no part of the thesis has been submitted in this form to any other institution of higher education for an academic degree.

Vienna, 30.05.2025

Solomiia Beska

For Lisa

— whose unwavering faith in me has been my quiet strength throughout this journey

TABLE OF CONTENTS

ABSTRACT

This dissertation examines Ukraine's evolving cyber resilience amidst protracted Russian cyber aggression and hybrid warfare from 2014 to 2025. It explores Ukraine's transformation from a vulnerable post-Soviet state to an emerging cyber-resilient actor amidst escalating digital threats, institutional weakness, and geopolitical uncertainty. The research question is twofold: How does a state become cyber resilient in the face of protracted cyber aggression? And was Ukraine's transformation driven by a pre-designed strategy or reactive learning through the crisis? The theoretical framework combines Peter Hall's (1993) theory of third-order policy change and Mark Basinger's (2002) model of national mobilization during times of crisis and upheaval. These theories define the "imperial puzzle" underlying the analysis: how state resilience emerges under external pressure through paradigm shifts and success-oriented imitation. Methodologically, the dissertation employs a longitudinal case study of Ukraine using process tracing and document analysis of official legislation, cyber strategies, incident reports, and institutional reforms. The study used MAXQDA to code and analyze primary indicators of the imperial puzzle. Empirical evidence suggests that Ukraine's resilience emerged through cumulative adaptation to shocks, such as the BlackEnergy attacks (2015), the NotPetya malware (2017), and the Kyivstar leak (2023), as well as limited adoption of Estonia's digital governance model. The dissertation proposes a three-stage model of resilience—evolution, progress, and development—demonstrating that Ukraine's cyber transformation was not centrally planned but rather emerged through institutional learning, strategic adaptation, and international cooperation. The proposed title of the dissertation is "Cyber Resilience in Ukraine: Measuring Response to Cyber Threats in the Context of Hybrid Warfare."

ACKNOWLEDGMENTS

This thesis marks the culmination of a deeply personal and intellectual journey, and I am profoundly grateful to all those who supported me along the way.

First and foremost, I would like to express my sincere gratitude to my supervisor, Professor Erin K. Jenne, for her intellectual guidance, steady encouragement, and thoughtful feedback throughout the research process. Her mentorship has been vital in shaping both the structure and substance of this project.

I would also like to express my heartfelt thanks to Dr. Vera Eliasova, Senior Lecturer at CEU's Center for Academic Writing. Her insightful guidance, patience, and unwavering support greatly strengthened my ability to express complex arguments clearly and persuasively. Her feedback not only improved my writing but also deepened my confidence in academic thinking and communication.

I also thank the faculty and staff of Central European University, particularly the Department of International Relations, for cultivating an intellectually stimulating and supportive environment during my studies.

I am deeply grateful to the Invisible University for Ukraine (IUFU), where I have had the privilege of serving as a mentor for the past three years. The IUFU program, through its unwavering commitment to supporting Ukrainian students affected by war, has been a space of hope, solidarity, and academic renewal. In particular, I would like to thank Professor Balázs Trencsényi, Director of the Institute for Advanced Study at CEU, whose inspiring dedication to academic freedom and transnational education encouraged me to apply to CEU in the first place. His mentorship and vision made this academic journey possible.

To my friends and colleagues from CEU and Ukraine—thank you for your solidarity, resilience, and shared purpose. Special appreciation goes to those working in the field of cybersecurity and public policy, whose work on the front lines has informed and inspired this research.

To my family—thank you for your unwavering love and support, especially during the most difficult moments. Your strength gave me the foundation to pursue this work.

Finally, I dedicate this thesis to Ukraine, whose ongoing struggle for sovereignty and digital resilience continues to guide my research and purpose.

Chapter 1: Defining Cyber Resilience: Conceptual Clarification and Analytical Distinction

"The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a "cyber Pearl Harbor:" an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."

— Leon E. Panetta, "Defending the Nation from Cyber Attack," speech, Business Executives for National Security, New York, October 11, 2012.

INTRODUCTION

In a now-famous speech in 2012, then–U.S. Secretary of Défense Leon Panetta warned that the next great national trauma might not come from land, air, or sea—but through cyberspace. By invoking the phrase "Cyber Pearl Harbor," Panetta painted a scenario where cyber actors launch synchronized attacks on critical infrastructure—electric grids, transportation systems, financial networks—alongside kinetic operations. The result, he cautioned, would not merely be data breaches or temporary disruptions, but real-world consequences: destruction, paralysis, and potentially loss of life. His warning marked a paradigmatic shift in how military and political leadership conceptualized modern security threats: the frontline had extended into the digital realm.

But now, more than a decade later, it is clear that these warnings were prophetic. When the Russian Federation invaded Ukraine more than three years ago, it was not just a territorial attack — it was also a digital attack. Cyberattacks were a pre-emptive setup for a large-scale invasion, accompanying traditional warfare by targeting Ukraine's mobile network, government

communications, official government websites and, most importantly, critical infrastructure.These operations are not isolated acts of sabotage, but rather part of a broader hybrid warfare strategy aimed at undermining state capacity, sowing confusion and weakening social cohesion. The *Extended Report: Cyber Conflict in Ukraine* (Thales, 2023, p. 13), provides a comprehensive overview of Russian cyberattacks as a well-planned tactic of cyberwarfare aimed at destabilising post-Soviet countries. The report provides a visual overview of major Russian-sponsored advanced persistent threat (APT) groups and their coordinated cyber operations over the past 15 years, illustrating that cyberattacks against former Soviet states, such as Estonia (2007), Georgia (2008) and Ukraine (since 2014), form part of an evolving, planned cyber warfare strategy. The report identifies specific cyber groups such as APT28 (Fancy Bear), APT14 (BlackEnergy) and UNC1151 (Gamaredon) and links them to areas of political tension.

Analyzing cyberattacks since 2007; we can conclude that their frequency has the potential to increase. Cybersecurity[1] has thus evolved from a niche technical concern into a core issue of international politics and strategic stability. Yet, while scholarly and policy attention has focused extensively on threats, attackers, and methods of deterrence, far less is known about the other side of the equation: how states build the capacity to absorb, recover from, and adapt to such threats. This thesis investigates that capacity so called "cyber resilience"—as both a conceptual innovation and an empirical reality.

[1] "Cybersecurity is defined in Ukrainian legislation as the protection of vital interests of individuals, society, and the state during the use of cyberspace, ensuring the sustainable development of the information society and digital environment, as well as the timely detection, prevention, and neutralization of real and potential threats to Ukraine's national security in cyberspace." See: *Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" No. 2163-VIII, adopted October 5, 2017, Article 1*, (my own translation)**.** See original text: Закон України "Про основні засади забезпечення кібербезпеки в Україні" № 2163-VIII від 5 жовтня 2017 року, стаття 1, визначає:
«Кібербезпека — це захист життєво важливих інтересів особи і громадянина, суспільства і держави при використанні кіберпростору, який забезпечує сталий розвиток інформаційного суспільства і цифрового середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України в кіберпросторі».

At the core of this thesis lies a simple yet pressing question: how does a state build cyber resilience not during times of stability, but under fire? While cyber resilience is widely referenced in NATO and EU doctrines, its development is often assumed to be the result of anticipatory planning and institutional strength. Ukraine, however, presents a "least likely" case. Entering the post-2014 period with weak institutions, fragmented legal frameworks, and limited resources, it nonetheless emerged as one of the most adaptive actors in modern cyber conflict. This thesis explores not only what cyber resilience is, but how it was built in wartime conditions.

A central contribution of this research is to show this cyber resilience not a result from a pre-designed outcome, but as a learning process. I argue that Ukraine's capacity to adapt emerged through critical junctures a series of the 2015 BlackEnergy attack, the 2017 NotPetya malware, and the 2023 Kyivstar breach—that triggered institutional transformation. Drawing on Peter Hall's (1993) theory of third-order policy change and Mark Beissinger's (2002) model of success-driven emulation, the thesis shows how Ukraine incrementally reshaped its cyber architecture in response to repeated shocks.

Within this process, Estonia served making it an example of cyber resilience as a referential model. Following its own 2007 cyber crisis, Estonia developed a robust cyber governance framework, becoming a leader in NATO-aligned cyber policy and legal innovation. Ukraine's reforms—such as the creation of CERT-UA, legal harmonization with the EU's NIS Directive, and the 2025 Law on Critical Infrastructure Protection—were not wholesale replications of Estonia's model[2] but bounded adaptations shaped by wartime constraints. By studying how

[2] Examples: "Ukraine will carry out a radical reform of the system of training and retraining of specialists in the field of cybersecurity, the state will stimulate research and development in the field of security of digital services," *National Cybersecurity Strategy of Ukraine 2021*, National Security and Defense Council of Ukraine, enacted by Presidential Decree No. 96/2021, March 2021. And second one "As a result of Russia's unprovoked war of aggression against Ukraine, the Tallinn Mechanism aims to coordinate and facilitate civilian cyber capacity building to help Ukraine uphold its fundamental right to self-defence in cyberspace, and address longer-term cyber resilience needs," *Tallinn Mechanism: Cyber Capacity Building for Ukraine*, 2024

Ukraine selectively emulated Estonia under pressure, the thesis contributes to understanding cyber resilience as a strategic, context-dependent, and iterative learning process.

In the context of hybrid warfare, digital systems have become both targets and weapons. State and non-state actors weaponize code, exploit vulnerabilities, and disrupt the delivery of critical services. Cyberattacks can paralyze hospitals, disable communications, falsify public records, and erode the legitimacy of political institutions. Yet in contrast to kinetic warfare, cyber aggression unfolds in a legal and strategic grey zone. The very nature of cyberspace—its speed, anonymity, and transnational reach—undermines traditional models of deterrence and attribution. As a result, the capacity to prevent cyberattacks is increasingly difficult to guarantee. It is precisely this shift—from prevention to endurance—that makes cyber resilience a vital to state security in the twenty-first century.

1.1 What Is Cyber Resilience?

Cyber resilience[3] refers to the ability of a system—technical, institutional, or societal—to anticipate, withstand, recover from, and adapt to adverse cyber events. Unlike cybersecurity, which emphasizes the protection of assets and the prevention of breaches, cyber resilience assumes that disruptions will occur and focuses instead on how to maintain core functions, recover rapidly, and evolve in the face of future threats (De Mauro et al. 2018; Munusamy and Khodadadi 2023).

This concept dithered from other concepts in several key ways. Cybersecurity is concerned primarily with defending digital infrastructure from unauthorized access, data breaches, and disruption—through encryption, firewalls, intrusion detection systems, and access controls. Cyber defense, in contrast, refers to the deployment of active, often military or intelligence-led capabilities to repel attacks, retaliate, or pre-empt adversarial actions—frequently coordinated at the national security level. Cyber deterrence, derived from Cold War nuclear strategy, seeks to prevent cyber aggression through threats of punishment or denial of benefit (Libicki 2009; Gartzke 2013).

Cyber resilience is fundamentally different. It does not rely on the illusion of perfect defense or on the rationality of deterrence. Rather, it embraces the inevitability of disruption and prioritizes continuity, flexibility, and learning. As Cavelty (2018, 133) explains, resilience is "a governance strategy that enables societies to manage uncertainty and complexity," often

[3] "Cyber resilience is defined in the 2021 Cybersecurity Strategy of Ukraine as the ability to quickly adapt to internal and external threats in cyberspace while ensuring the stable functioning of national information infrastructure, especially critical infrastructure." See: Cybersecurity Strategy of Ukraine, approved by Presidential Decree No. 447/2021, August 26, 2021, (my own translation). See original: Указ Президента України № 447/2021 від 26 серпня 2021 року, яким затверджено Стратегію кібербезпеки України, визначає: «Кіберстійкість — це здатність швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, забезпечувати стабільне функціонування національної інформаційної інфраструктури, особливо критичної інформаційної інфраструктури».

through decentralized, multi-actor, and cross-sectoral coordination. It reflects a systemic shift from protecting the perimeter to sustaining the mission.

Scholars such as Dunn Cavelty and Wenger (2023) have stated that cyber resilience entails not only technical preparedness but also behavioural, institutional, and legal transformation. Resilience is both a process and a capacity—it is cultivated over time through institutional learning, organisational adaptation, and policy feedback. Milanova (2020,68-69) alls this "learning under stress" and defined as "the ability of states and societies to reform, thus withstanding and recovering from internal and external crisis", highlighting how institutions evolve in response to real-world crises rather than pre-designed strategies.[4]

Conducting a legislative and doctrinal analysis of key international legal instruments and strategic documents, I have found that cyber resilience is increasingly defined as a multidimensional capability—intersecting the legal, technical, institutional, and societal domains. This understanding moves beyond the narrow conceptualization of resilience as a reactive technical fix, and instead situates it within a broader political and normative framework In NATO's Strategic Concept and resilience guidelines adopted at *Strengthened Resilience Commitment* (NATO 2021), "rresilience is a national responsibility and a collective

[4] "Operationally, Ukraine's cybersecurity doctrine requires all actors within the national system to respond to cyber incidents timely and effectively, maintaining constant readiness to both real and potential cyber threats. This includes creating incident management systems and training qualified personnel." See: *Cybersecurity Strategy of Ukraine, Decree No. 447/2021*, (for my own translation Ukrainian language). See original text: розділ 5. Пріоритети забезпечення кібербезпеки України та стратегічні цілі», підпункт К.1. Національна кіберготовність та надійний кіберзахист, зазначено:
«Україна посилить кіберготовність, що полягатиме у здатності всіх заінтересованих сторін, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення, забезпечивши тим самим кіберстійкість, передусім об'єктів критичної інформаційної інфраструктури. Україна створить національну систему управління інцидентами». And NATO, for instance, frames cyber resilience as the capacity to deter, defend against, and always recover from cyber threats—during peace, crisis, and conflict—through coordinated efforts at the political, military, and technical levels (NATO 2021).

commitment" and cyber is treated as both a standalone domain and an enabler of collective defence, necessitating whole-of-government preparedness and international interoperability.

Similarly, the European Union advances a preventive approach to cyber resilience. The Cyber Resilience Act (CRA), adopted in 2022, aims to establish horizontal cybersecurity requirements for digital products, recognizing that systemic vulnerabilities arise not only from threat actors but also from fragmented governance and insufficient legal accountability (European Commission 2022). In parallel, the Joint Cyber Unit initiative emphasizes the need for cross-border coordination in responding to large-scale cyber incidents, highlighting the fusion of resilience with both crisis management and digital sovereignty (ENISA 2023). These frameworks collectively signal a paradigm shift: cyber resilience is no longer seen as a purely technical or operational task, but rather as a strategic function embedded in national security policies, digital legislation, and transnational institutional cooperation.

This evolution is particularly evident in the way international organizations embed resilience into their legal and policy narratives. Resilience becomes not only a measure of recovery capacity, but also a test of institutional learning, adaptability, and democratic legitimacy in the digital age. As such, it is increasingly treated as a legal-political norm—anchored in preparedness, deterrence, and the ability to maintain societal continuity in the face of hybrid threats. In the case of Ukraine, as will be shown in subsequent chapters, this conceptual and institutional evolution has played a crucial role in shaping its national cybersecurity architecture and strategic doctrine under conditions of protracted cyber aggression.

To unpack how this multidimensional understanding of cyber resilience has evolved, it is necessary to analyse several key international legal and policy instruments that shape contemporary approaches to digital security. These documents illustrate the gradual shift from a reactive cybersecurity model to a proactive, system-wide framework of resilience.

*The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (*Schmitt 2017)[5] remains the most comprehensive attempt to interpret how existing international law applies to cyber operations, particularly in the context of sovereignty, due diligence, and armed conflict. While not legally binding, the Manual introduces the concept of "resilience" as the obligations of to prevent their territory from being used for harmful cyber operations. It also reinforces the idea that cyber resilience involves both defensive capacity and legal responsibility in deterring hostile acts originating from national infrastructure.

The United Nations Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (2010–2021) have produced several consensus reports that affirm the applicability of the UN Charter in cyberspace and articulate voluntary norms of responsible state behavior. Among these, the duty to exercise due diligence, protect critical infrastructure, and cooperate in incident response are framed as key components of a cyber-resilient international order (UN GGE 2015; OEWG 2021). These reports suggest that cyber resilience is not merely a domestic task, but also an emerging norm in international peace and security.

The Preamble of the Budapest Convention on Cybercrime (Council of Europe 2001) "recognising the need for co-operation between States and private industry in combating cybercrime" - provides the foundational legal instrument for harmonizing domestic criminal laws related to cybercrime and establishing channels for international cooperation (Article 36,37). While focused on criminal justice, its structure promotes a form of legal resilience by

[5] Although the *Tallinn Manual 2.0* does not define cyber resilience as a standalone legal concept, it implicitly frames it through the principles of sovereignty (Rules 1–4), the obligation of due diligence (Rule 6), and the prohibition against violating other states' sovereignty (Rule 4). These norms together provide a legal basis for understanding cyber resilience as a state's capacity to regulate, protect, and respond to cyber threats under international law. See *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. Michael N. Schmitt (Cambridge: Cambridge University Press, 2017).

creating interoperable investigative mechanisms and legal standards. The Convention's growing list of signatories—including Ukraine—illustrates how legal harmonization serves as a tool of institutional resilience and mutual defense against transnational threats.

At the regional level, the EU's Network and Information Security Directive (NIS2), adopted in 2022, expands upon its predecessor by imposing stricter obligations on essential and important entities in sectors such as energy, health, and digital infrastructure. NIS2 explicitly links cybersecurity to resilience, requiring risk-based security policies, incident response plans, and accountability frameworks. In parallel, the Cyber Resilience Act (CRA) introduces horizontal cybersecurity requirements for digital products and services, thereby embedding resilience principles into the EU's regulatory fabric (European Commission 2022). These instruments reflect the EU's move from the reactive handling of tacks to preventive, governance-driven cyber resilience.

Internationally, the NIST Cybersecurity Framework developed in the United States (2018) and the U.S. National Cybersecurity Strategy (2023) both operationalize resilience as a central pillar of national defense and economic stability. The NIST framework promotes a risk-based approach with five functions—Identify, Protect, Detect, Respond, Recover —that are widely adopted as international standards. The 2023 strategy, in turn, stresses principles, preemptive threat disruption, and public-private coordination, positioning cyber resilience as a geostrategic imperative.

Additionally, soft-law instruments such as the OECD Recommendations on Digital Security Risk Management (2015, revised 2019) reinforce resilience by emphasizing institutional learning, multistakeholder cooperation, and proportionality in risk governance.

In sum, Ukraine's evolving cyber capabilities reflect a shift from ad hoc responses toward institutionalized cyber resilience. As part of my analysis, I will closely examine the 2021

Cybersecurity Strategy of Ukraine (enacted by Presidential Decree No. 96/2016) and the recently adopted Law No. 4336-IX (2024, effective 2025). These legal instruments will be analyzed to trace whether and how they embody a learning process and alignment with EU/NATO standards. The Strategy outlines national coordination through the National Cybersecurity Coordination Center and emphasizes the development of a risk-based, preventive cybersecurity system, the new law introduces concrete procedures for protecting critical infrastructure and managing cyber vulnerabilities. By studying these texts, I aim to assess the extent to which Ukraine's cyber resilience is being framed as both a matter of national survival and a pathway to international integration.[6]

Crucially, cyber resilience operates within a legal and strategic "grey zone." Cyberattacks often fall below the threshold of armed conflict, and their attribution is frequently ambiguous. The International Committee of the Red Cross (ICRC) has stated that cyberspace is increasingly exploited for military operations that evade traditional legal categories, raising concerns about civilian infrastructure, proportionality, and the distinction between military and civilian targets (ICRC 2020, 486–89). In this context, resilience stated not only a system level safeguard but also a normative commitment to governance amid uncertainty.

Together, these legal and policy frameworks illustrate the emergence of cyber resilience as a normative, institutional, and strategic concept. It is not simply about withstanding attacks but

[6] Law of Ukraine No. 4336-IX "On Amendments to Certain Laws of Ukraine on Information Protection and Cybersecurity of State Information Resources and Critical Information Infrastructure," adopted March 27, 2025. See especially the updated Article 8: "Державні інформаційні ресурси […] мають оброблятися в авторизованих системах з безпеки або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки"
Presidential Decree of Ukraine No. 96/2021, "On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021, 'On the Cybersecurity Strategy of Ukraine,'" enacted on August 26, 2021. The Strategy states: "Key objectives include ensuring the readiness of national cybersecurity system actors to respond to cyber incidents, strengthening coordination mechanisms [...], and implementing a unified cyber incident management system (my own translation). See original text : Указ Президента України №96/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"», від 26 серпня 2021 року. Цитата: «Основними завданнями є забезпечення готовності суб'єктів національної системи кібербезпеки до реагування на кіберінциденти та кіберінциденти, посилення координації дій […] та запровадження єдиної системи управління кіберінцидентами»

about cultivating the legal, organizational, and societal conditions that allow systems to adapt, learn, and recover in a complex threat environment.

In so far as the concept of cyber resilience is a multidimensional phenomenon, it becomes necessary to determine how this resilience can be measured and how the cyber resilience of a state can be credibly asserted.

Because cyber resilience is multi-dimensional and dynamic, it cannot be measured by a single indicator. Instead, it requires a comprehensive framework encompassing several interrelated dimensions. These include:

First, a legal and regulatory framework consisting of updated cybersecurity legislation, clearly defined national strategies, and compliance with international standards, such as the EU NIS2 Directive and the General Data Protection Regulation (GDPR), is essential to building institutional cyber resilience and capacity for legal adaptation in times of crisis (Shaffique, 2024; Milanova, 2020).

Second, institutional capacity, which encompasses the operational maturity and effectiveness of national Computer Emergency Response Teams (CERTs) and Cybersecurity Incident Response Teams (CSIRTs), coordination between governmental agencies, prioritization of cyber-related budgets, leadership awareness, and the ability to respond collectively to incidents (Rahman and Cachia 2021).

Third, technical infrastructure, which involves embedding resilience-by-design principles into national and private digital ecosystems, ensuring system redundancy, deploying secure data storage and recovery protocols, and utilizing threat-monitoring technologies (Shaw et al. 2022; ENISA 2022).

Fourth, societal mobilization, which is reflected in national efforts to raise digital literacy, promote cyber hygiene through public campaigns, and facilitate the active participation of civil

society and private actors in digital security and emergency response frameworks (Berkes and Ross 2013; Papakonstantinou 2022).

Fifth, international cooperation, which refers to the degree of engagement in transnational cyber defense alliances, the exchange of threat intelligence across borders, and the integration into structures such as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the EU Cyber Solidarity Act, and the UN Open-ended Working Group on responsible state behavior in cyberspace.

Thus, cyber resilience reflects a state's ability to defend itself in cyberspace and govern through disruption. It means maintaining critical functions, public trust, and adapting institutions to constant pressure while evolving constantly. As threats grow, today's resilience may not be sufficient tomorrow.

Crucially, the concept of cyber resilience is descriptive, not explanatory. It describes what a state or system is capable of doing in response to cyber threats—but not how that capacity emerges. This thesis seeks to understand it emerges. To do so it adopts cyber resilience as the dependent variable and seeks to explain how it can develop under conditions of sustained cyber aggression, I show that it emerged in Ukraine through the processes of learning, adaptation, and emulation.

The field of cybersecurity has undergone rapid theoretical and empirical expansion over the past two decades, yet one concept remains insufficiently theorized: cyber resilience. While scholars have long debated whether state cybersecurity strategies should prioritize deterrence, defense, or regulation, these frameworks tend to emphasize static, pre-engineered approaches that overlook the dynamic processes through which resilience is actually developed—particularly in states under sustained attack.

In classical treatments, cybersecurity is often portrayed as a function of rational planning. Libicki and Rid, for instance, analyze cyber operations through the lens of deterrence and offensive doctrine, focusing on state capabilities, threat modeling, and countermeasures (Libicki 2009; Rid 2013). Carr and Streltsov contribute legal and institutional perspectives, centering on normative frameworks, regulatory harmonization, and internet governance (Carr 2016; Streltsov 2017). The literature here assumes that states achieve cyber stability by designing robust policies in advance—often drawing from military doctrine or legal precedent. However, such models struggle to explain how resilience emerges in fragile, war-affected, or post-Soviet contexts. They treat cyber resilience as a product—a final stage of well-designed governance—rather than as a process. This narrow framing misses the critical question: how is resilience actually built when a state lacks the time, capacity, or consensus for ex ante policy design?

A newer strand of scholarship begins to address this gap. Barnea, Weiss, and Shemer (2020) conceptualize resilience as a multidimensional capability that involves not only technological robustness but also political adaptability and societal cohesion. Eichensehr adds that in wartime settings, cyber resilience should be viewed as a constitutional defense mechanism, encompassing infrastructure, policy, and public trust (Eichensehr 2022). Topor emphasizes that cyber resilience intersects with sovereignty and legitimacy, particularly under conditions of hybrid war and information manipulation (Topor 2024). These works mark a shift from treating resilience as a technical checklist to seeing it as a political process. This reconceptualization is mirrored in policy frameworks. The EU Cyber Resilience Act, NATO's evolving doctrine, and the ENISA Cyber Threat Landscape increasingly frame resilience as a strategic objective, particularly in the domain of critical infrastructure protection (European Commission 2022; Štitilis, Malinauskaitė, and Pakutinskas 2017; Fotescu et al. 2021). Bendiek and Maat further argue that resilience is now central to EU foreign and defense policy (Bendiek and Maat 2021).

Yet while these initiatives offer legal blueprints and technical standards, they remain largely normative and aspirational. Few provide empirical accounts of how resilience emerges under sustained cyber pressure or amid institutional fragility.

Estonia is often held up as the most successful example of national cyber resilience. Following the 2007 cyberattacks attributed to Russia, Estonia rebuilt its digital architecture, created CERT-EE, and helped establish NATO's CCDCOE (Ottis 2008; Herzog 2017). This led to the development of the Tallinn Manual, a foundational document in cyber law. Scholars widely cite Estonia as a benchmark for cyber preparedness and adaptation. Yet its trajectory unfolded in peacetime, within the framework of EU accession with high levels of institutional consensus—conditions not replicable in Ukraine.

By contrast, Ukraine—despite being the most targeted state in modern cyber warfare—remains underexplored in both the academic and policy literatures. Since 2014, Ukraine has faced a wave of escalating cyber incidents: the BlackEnergy Led to attack on the energy grid in 2015, the NotPetya malware campaign in 2017, and the systemic disruption of Kyivstar during wartime in 2023. These shocks were not only technical threats but political turning points. They exposed institutional vulnerabilities and forced reactive, often improvised reforms. Yet existing studies primarily provide threat assessments or technical diagnostics, rather than theoretical accounts of how resilience was built (SSSCIP 2023, 2024; CERT-UA 2023, 2024; Microsoft 2023; Canadian Centre for Cyber Security 2022).

This thesis adresses that gap. It moves beyond Estonia's peacetime model and questions whether resilience must always precede crisis—or whether, as in Ukraine's case, it can emerge through crisis. Drawing on Peter Hall's "theory of third-order policy change", it argues that Ukraine's resilience evolved through critical junctures that transformed not only institutions but strategic priorities (Hall 1993). In line with Beissinger's model of learning under external

pressure, it further demonstrates how Ukraine emulated Estonia's frameworks—CERT-UA, the 2017 and 2025 cybersecurity laws, and NATO-aligned strategy documents—not through duplication, but bounded adaptation (Beissinger 2002).

The few studies that examine resilience as a process rather than a condition remain fragmented. Perez, Bocanet, and Sallos explore organizational resilience but stop short of theorizing its political dimensions (Perez, Bocanet, and Sallos 2024). Gilardi et al., Meseguer, and Dobbin, Simmons, and Garrett contribute policy diffusion frameworks that illuminate how states learn from others—but do not explain how war shapes emulation patterns (Gilardi et al. 2009; Meseguer 2005; Dobbin, Simmons, and Garrett 2007). Meanwhile, works like Tasheva, Tiirmaa-Klaar, and Chiara and Brighi begin to link resilience with hybrid warfare and EU law, yet lack empirical depth in frontline cases (Tasheva 2021; Tiirmaa-Klaar 2024; Chiara and Brighi 2024). Ukraine's case reveals the need to move from static to dynamic models of resilience. It calls for a theoretical shift—from resilience as design to resilience as learning. This includes recognizing not only institutions and infrastructure, but also civilian mobilization (e.g., the IT Army), cross-sector alliances (e.g., USAID and NATO cooperation), and the political narratives that sustain public trust in digital sovereignty.

To summarize, the reviewed literature highlights several important gaps that motivate this research. First, there is limited empirical analysis of how cyber resilience is actually built under conditions of sustained conflict and institutional disruption. Second, many existing studies rely heavily on anticipatory or rationalist models, which may overlook the importance of reactive learning and adaptation in real-time crises. Third, Ukraine—despite being the most persistently targeted state in modern cyber conflict—remains significantly underrepresented in academic accounts of resilience-building processes.

I explore whether a learning-based model—grounded in institutional responses to cyber shocks, strategic adaptation, and bounded emulation of external examples—offers a more plausible account of Ukraine's evolving cyber resilience between 2014 and 2025.Moreover, influential conceptual frameworks further refine this thesis's core assumption: that cyber resilience is not simply a product of defense, but a process of institutional and societal endurance. Resilience means managing failure rather than preventing all attacks—it involves the maintenance of essential functions and trust in governance systems under cyber stress (Dunn Cavelty 2018). Resilience is the strategic blending of defense, recovery, and adaptability—particularly when deterrence fails (Atrews 2020). It is a four-phase process—anticipate, absorb, recover, and adapt—that informs legal frameworks like the EU Cyber Resilience Act (Shaffique 2024). Organizational and societal readiness, integrity under pressure, and the ability evolve are essential pillars of this model (Munusamy and Khodadadi 2023; Milanova 2020). As these perspectives show, Ukraine's experience cannot be captured by static, pre-defined notions of cybersecurity or defense. Instead, cyber resilience emerges through improvisation, public-private coordination, regulatory adaptation, and strategic foresight—all of which are central to the Ukrainian response.

1.2 Research Question and Puzzle

This thesis addresses a foundational problem at the intersection of international security, crisis adaptation, and digital governance: How do states become cyber-resilient under conditions of sustained cyber aggression? More specifically, it asks: How has Ukraine developed cyber resilience in response to Russian cyberattacks since 2014, and to what extent has this transformation been shaped by institutional learning, strategic adaptation, and bounded policy emulation—particularly of Estonia's post-2007 reforms?

This thesis addresses a critical puzzle in international relations and cybersecurity: How does cyber resilience emerge in states under conditions of hybrid warfare, particularly when institutional capacity is limited and strategic planning is constrained? Ukraine represents an especially compelling case. Despite being the most persistently targeted country in modern cyber conflict since 2014, it has demonstrated an evolving capacity to absorb, respond to, and adapt to digital threats. This is puzzling because Ukraine had fragmented institutions, outdated legal frameworks, and minimal anticipatory at the outset of the war.

Cyber resilience has been conceptualized. While widely referenced in EU and NATO policy documents, cyber resilience remains under-theorized in academic literature, especially in conflict-affected or transitional states. Most existing studies treat it as either a technical capability (focused on infrastructure and systems) or a static posture of response and recovery.

This thesis offers an alternative. Talk about its adaptability concept of cyber resilience is not simply an end-state or engineered outcome, but rather a dynamic, learning-driven process—shaped by repeated cyber shocks, institutional improvisation, and bounded emulation of successful models such as Estonia.

Because as Ukraine's Ministry of Foreign Affairs (2025) states "The world's response to Russian aggression will define global security and economic architecture for many decades to

come. In today's interconnected digital world, where cyber threats know no borders, we can only achieve sustainable and timely outcomes through coordinated efforts, capacity building, mutual learning, experience sharing, public-private partnerships and joint initiatives." (Ministry of Foreign Affairs of Ukraine 2025)

Building on this insight, I introduce a learning-based model of cyber resilience. It conceptualizes resilience as an emergent property of three interlinked mechanisms: institutional learning, strategic adaptation, and selective emulation of external frameworks under pressure. Ukraine's post-2014 experience, I contend, provides a "hard test" for this model—a context where resilience is least likely to develop, yet where it has in fact emerged.

This research question emerges from both a theoretical and empirical puzzle. Theoretically, the dominant literature assumes that cyber resilience results from ex ante planning and rational institutional design. In these accounts, states adopt strategies, build infrastructure, and enact legal frameworks in anticipation of future threats (Dunn Cavelty 2018; Deibert 2013). However, such models presume stable conditions and foresight—conditions absent in many transitioning or conflict-affected states.

In fact, often in various forms emerge crisis settings. Following the annexation of Crimea in 2014, Ukraine entered a hostile digital environment with limited institutional capacity. The Computer Emergency Response Team of Ukraine (CERT-UA), established in 2007, had a narrow mandate and minimal operational capacity. The country's legal framework, based on the 2003 Law on National Security and the 2006 Law on the State Service of Special Communications and Information Protection, offered little strategic coherence. Cybersecurity remained embedded in older notions of "information protection," with no integrated cyber defense strategy.

Despite this, Ukraine has become one of the most tested and adaptive cyber actors in Europe. Major cyber incidents—including BlackEnergy (2015), NotPetya (2017), the Viasat satellite attack (2022), and the Kyivstar breach (2023)—were not isolated, but components of a sustained hybrid campaign. Each exposed deep systemic vulnerabilities, but also triggered institutional reform and strategic innovation. This paradox—how a state with weak starting capacity built resilience under wartime conditions—forms the core of my empirical puzzle.

Most existing scholarship is poorly equipped to answer this question. Resilience is typically framed as the outcome of anticipatory governance, where institutions forecast risk and prepare accordingly. This thesis offers an alternative: resilience as an emergent capacity, produced through iterative adaptation and learning under pressure. Drawing on Peter Hall's (1993) theory of third-order policy change, I argue that Ukraine's resilience emerged through repeated cyber shocks that acted as critical junctures, leading to strategic shifts in legal frameworks, institutional arrangements, and governance practices.

My theoretical framework drives on Mark Beissinger's (2002) model of success-driven learning in the case of Ukraine.

To avoid tautological reasoning and enhance analytical precision, I disaggregate the broader process of resilience-building into three embedded mini-cases—each corresponding to a distinct cyber shock that triggered institutional and strategic responses: the BlackEnergy attacks on Ukraine's energy grid in 2015, the NotPetya malware campaign in 2017, and the 2023 breach of the Kyivstar mobile network.

Each case represents a decision-making episode where Ukrainian institutions were forced to respond, often improvisationally, and often looking to external models such as Estonia. These episodes are analyzed through process tracing, contrasting observed institutional responses with

their consequences use not: Did Ukraine's policy shifts reflect rational cost-benefit calculations from a blank slate, or were they shaped by reactive learning and bounded emulation?

My research employs an evidentiary signature and a longitudinal case structure, which allows for comparative inferences over time. Ukraine's trajectory provides a unique opportunity to examine how cyber resilience can emerge amidst connected institutional fragility, continuous cyber assault, and uncertain international support. Its success challenges linear models of resilience based on institutional strength and planned governance.

Theoretically, this research contributes to broader debates on how states adapt under hybrid warfare and institutional stress. It offers an account of resilience as socially embedded, reactive, and externally referenced—rather than engineered in advance. Practically, Ukraine's example offers relevant lessons for conflict-affected states and post-Soviet democracies navigating the uncertain terrain of cyber conflict.

In sum, this thesis provides a dynamic and empirically grounded answer to a strategic puzzle: How can cyber resilience be built not before the storm—but through it

1.3 Argument, Theory, and Conceptual Framework

This thesis explores two competing theoretical models to explain how cyber resilience emerges in a state under sustained digital aggression. Rather than beginning with a preselected framework, the study adopts a theory-testing approach to evaluate whether Ukraine's cyber resilience has developed primarily through anticipatory rational planning or through reactive adaptation and bounded emulation. The case of Ukraine serves as a "hard test" for both approaches, given the intensity of cyber threats the state has faced since 2014.

The first theoretical model is rooted in rationalist traditions within international relations and policy studies. It assumes that states are strategic actors that design cybersecurity frameworks ex ante—before crises occur—based on cost-benefit calculations, threat assessments, and institutional foresight. Under this model, cyber resilience is understood as a product of proactive governance: policymakers are expected to construct legal frameworks, allocate resources, and build operational capacity in anticipation of cyber risks (Libicki 2009; Gartzke 2013). Applied to Ukraine, this would imply the presence of strategic doctrines, early institutional investment, and coherent cyber planning prior to major cyberattacks.

The second model draws on theories of learning and institutional adaptation. In particular, it builds on Peter Hall's (1993) concept of third-order policy change and Mark Beissinger's (2002) model of success-driven emulation. This framework holds that states often develop resilience not through prior planning but in response to crisis. Cyber incidents are treated as critical junctures—shocks that expose systemic weaknesses and trigger reactive reform. Under conditions of uncertainty and resource scarcity, states may selectively adopt elements of perceived successful foreign models. This process, known as bounded learning, involves emulating external frameworks—such as Estonia's cyber architecture—not through comprehensive design, but through constrained, adaptive appropriation.

This paper provides an explanation of Hall and Beissinger's theories and a narrative of their empirical data based on a comparative analysis of the theoretical foundations in the MAXQDA program and the empirical reflections in the primary documents studied. Hall distinguishes three types of policy learning: first-order (adjustment of instruments), second-order (change of political methods), and third-order changes, which denote a paradigm shift—a fundamental rethinking of policy goals, assumptions, and instruments. During my analysis, I found that third-order changes typically occur during critical periods when the dominant paradigm is no longer viable and decision-makers must reconsider fundamental assumptions. This adaptation most closely reflects the Ukrainian model. Hall explains that these changes are caused by a crisis, characterized by the breakdown of institutional procedures, the accumulation of political failures, and the emergence of new discourses and actors in the political sphere. Analogous to primary sources, my analysis demonstrates that Ukraine's cyber trajectory empirically offers strong evidence of such paradigm shifts. The NotPetya attack in 2017 marked a fundamental shift in perception of the state. What was previously considered a technical IT problem was reclassified as a national security issue, with serious legislative and institutional implications. The November 2022 attack on Ukraine's Ministry of Finance and the 2023 large-scale data leak from the Kyivstar network illustrate how upheavals lead to ad hoc policy experiments, redistribution of bureaucratic powers, and ultimately, the incorporation of cybersecurity into broader strategic planning—the very kind of institutional upheavals and transformations that Hall's theory anticipates. This is confirmed by documents such as the "Cybersecurity Strategy of Ukraine," updated in 2021 and revised again after 2022; the creation of new institutional actors, such as the National Cybersecurity Coordination Center (NCCCC); and Ukraine's full membership in the NATO Cooperative Cyber Defense Center of Excellence (NATO CCDCOE).

Mark Beissinger (2002) highlights how successful actions in other contexts can inspire imitation strategies. He shows that when faced with uncertainty, actors often respond to transformative events by adopting strategies that have "worked" in similar situations, even if only imperfectly. According to Beissinger, emulation driven by success clusters over time and triggers mobilization processes. Crisis events become the impetus for actors to change their identity and strategy. This institutional adaptation is twofold: reactive and selective. Actors imitate only what seems viable within their specific constraints—a process scholars call constrained learning (Meseguer, 2005).

Rather than treating either model as definitive, this thesis empirically tests both through a comparative analysis of three embedded case episodes: the Ukrainian state's responses to the BlackEnergy attack (2015), the NotPetya malware incident (2017), and the Kyivstar mobile network breach (2023). These episodes serve as discrete decision-making moments within a broader longitudinal process. Using process tracing and document analysis, I evaluate whether each response aligns more closely with the rationalist model—marked by proactive, cost-effective planning—or with the learning-based model—characterized by reactive reform and strategic emulation.

This study treats cyber resilience as the dependent variable, conceptualized as a multidimensional condition involving legal preparedness, institutional capacity, technical robustness, and societal engagement. The goal is not only to trace how Ukraine has become cyber-resilient, but to explain the causal logic behind that transformation. In doing so, the thesis contributes to broader debates in international relations about institutional change, governance under pressure, and the mechanisms of learning in crisis.

By juxtaposing these theoretical frameworks and applying them to sequential cyber crises in Ukraine, the thesis seeks to clarify how cyber resilience is actually built—not in theory, but in

practice. The study thus contributes to both conceptual development and empirical understanding of resilience in the context of hybrid warfare.

1.4 Rationalist Theory in International Relations and Its Application to Cybersecurity

In international relations, rationalist theory—often associated with neorealism or rational institutionalism—refers to an approach that explains state behavior as s function of strategic calculations of interests, threats, and benefits. It is typically contrasted with constructivist or critical approaches.

Analyzing this theory, one can assume that states are viewed as rational actors seeking to maximize their interests. They formulate policies, including cyber policies, *ex ante*—that is, in advance—based on strategic calculations. Their behavior is thus explained through the structure of the international system (anarchy, balance of power).

Accordingly, the rationalist approach assumes that states design cybersecurity strategies based on a logic of threats and gains. They do not wait for crises to erupt; rather, they act preventively. In this context, cyber resilience is conceived not as a product of adaptation or learning, but as a calculable requirement derived from defense planning. Testing this theoretical perspective, one would expect states to form cybersecurity strategies *ex ante* based on cost-benefit analysis, risk management, strategic assessment, and technocratic planning. In this logic, cyber resilience is an engineered and pre-designed product, not an outcome of post-crisis learning.

As Waltz (1979), Keohane (1984), and Fearon (1995) argue, states behave as rational actors that strategically pursue their survival and security. From this vantage point, cyber resilience is not seen as an emergent or adaptive response to crisis, but rather as a preplanned architecture—developed through threat anticipation, strategic calculus, and cost–benefit analysis.

In cybersecurity, this logic manifests through policy frameworks that prioritize predictive risk assessment, optimized institutional architecture, and long-term investments in cyber defense capabilities. In reviewing the literature, it becomes evident that rationalist interpretations include, for example, Martin Libicki's (2009) model of cyber deterrence, which parallels

nuclear deterrence and assumes planned development of state cyber capabilities. His framework represents a conceptual model of cyber defense potential. Libicki argues that cyber deterrence is challenging yet feasible under conditions of institutional planning. His multi-layered model—semantic, syntactic, and physical—emphasizes the necessity of preventive cyber defense. This vision reflects a rationalist strategic framework: hierarchy, standardization, and calculable threats.

Similarly, Erik Gartzke (2013) argues that cyber capabilities have limited strategic utility unless embedded in broader calculations of national power. He contends that political science in IR should aim to "demystify" (Gartzke 2013, 42) the panic surrounding cyberwarfare. His core idea is that cyber conflict has limited political effectiveness without material impact. From a rationalist viewpoint, Gartzke assumes that states act when benefits outweigh risks—there is no logic of consequences without force projection, making cyberwar unlikely in the absence of ground power.

Thomas Rid (2013), in turn, challenges the very concept of "cyberwarfare." He argues that most cyber operations fall under sabotage, espionage, or subversion, rather than war in the traditional sense. He claims that cyberattacks may in fact reduce physical violence by offering states an alternative, non-lethal tool of influence. While Rid does not fully adhere to rationalism, many of his arguments rest on strategic logic. He views cyber operations as instrumental tools that states deploy to achieve political objectives with minimal costs. He further suggests that states act rationally when choosing cyber instruments over conventional military force when the former is more advantageous.

If this rationalist logic were applicable to Ukraine, one would expect a sequence of ex ante developments: early threat identification, dedicated budgetary allocations, coherent strategic frameworks, and gradual institutional maturation in the field of cybersecurity. To test this

model, I conducted an empirical analysis combining process tracing and document analysis of budgetary, legislative, and institutional data from 2007 to 2025. I reviewed Ukraine's national budgets to trace financial commitments to cybersecurity; examined key legislative acts, including Law No. 2163-VIII (2017) and draft Law No. 11290 (2025); analyzed national cybersecurity strategies from 2016 and 2021; and evaluated the institutional outputs of the State Service of Special Communications and Information Protection (SSSCIP), the Computer Emergency Response Team of Ukraine (CERT-UA), and international partners such as NATO and Microsoft.

This investigation produced results that diverge significantly from rationalist expectations. Prior to 2014, Ukraine had no comprehensive cybersecurity strategy, no institutional infrastructure with operational authority, and no substantial budgetary allocations for cyber defense. CERT-UA, established in 2007, remained functionally inactive, with minimal integration into national defense planning. Cybersecurity was not prioritized in state budgets between 2007 and 2013. Strategic planning was virtually absent, and cyber policy was politically marginal.

A decisive shift occurred only after the onset of hybrid warfare. The BlackEnergy attack in 2015 and the NotPetya attack in 2017 became catalytic shocks that prompted the formulation of Ukraine's first cybersecurity strategy (2016) and the adoption of Law No. 2163-VIII (2017). These initiatives were not designed in anticipation of cyber threats but as reactive institutional responses to already materialized crises. A similar pattern repeated following the 2022 full-scale invasion and especially the 2023 cyberattack on Kyivstar, which triggered the development of draft Law No. 11290 (2025). These reforms consistently occurred *after* attacks, not before them.

Financial commitments to cybersecurity followed the same reactive pattern. Budget analysis indicates that significant funding for cyber defence appeared only after 2015 and increased sharply after 2022, contradicting rationalist assumptions of proactive resource allocation. Reports from SSSCIP and CERT-UA confirm that institutional scaling and technical capacity-building were implemented in crisis mode, driven by immediate mitigation needs rather than strategic foresight (CERT-UA 2023–2025; SSSCIP 2024).

Moreover, institutional learning occurred through bounded emulation rather than strategic optimization. Drawing on Beissinger's (2002) model of success-based emulation, Ukraine selectively adopted elements of Estonia's post-2007 cyber reforms, especially in its approach to CERT operations, legal harmonization with the EU's NIS Directive, and cooperation with NATO's CCDCOE. These emulations were selective, reactive, and often improvised. Peter Hall's (1993) concept of third-order change is also applicable: Ukraine did not merely adjust policy tools, but fundamentally redefined paradigms in response to crises, abandoning about information security and centralizing cyber governance.

Thus, the accumulated evidence undermines the explanatory power of rationalist theory in the Ukrainian context. Rather than being the product of premeditated cyber policy design, Ukraine's cyber resilience emerged from moments of institutional improvisation, shock-induced learning, and adaptive emulation. Rationalist models—though valuable in understanding policy design in stable and technically mature environments—fail to capture the contingency, fragmentation, and urgency that shaped Ukraine's cybersecurity trajectory. This case, therefore, supports learning-based explanations over rationalist planning paradigms in analyzing cyber resilience under conditions of hybrid warfare.

1.5 Learning-based model of Cyber Resilience and my model of Cyber Resilience: Evolution → Progression → Development

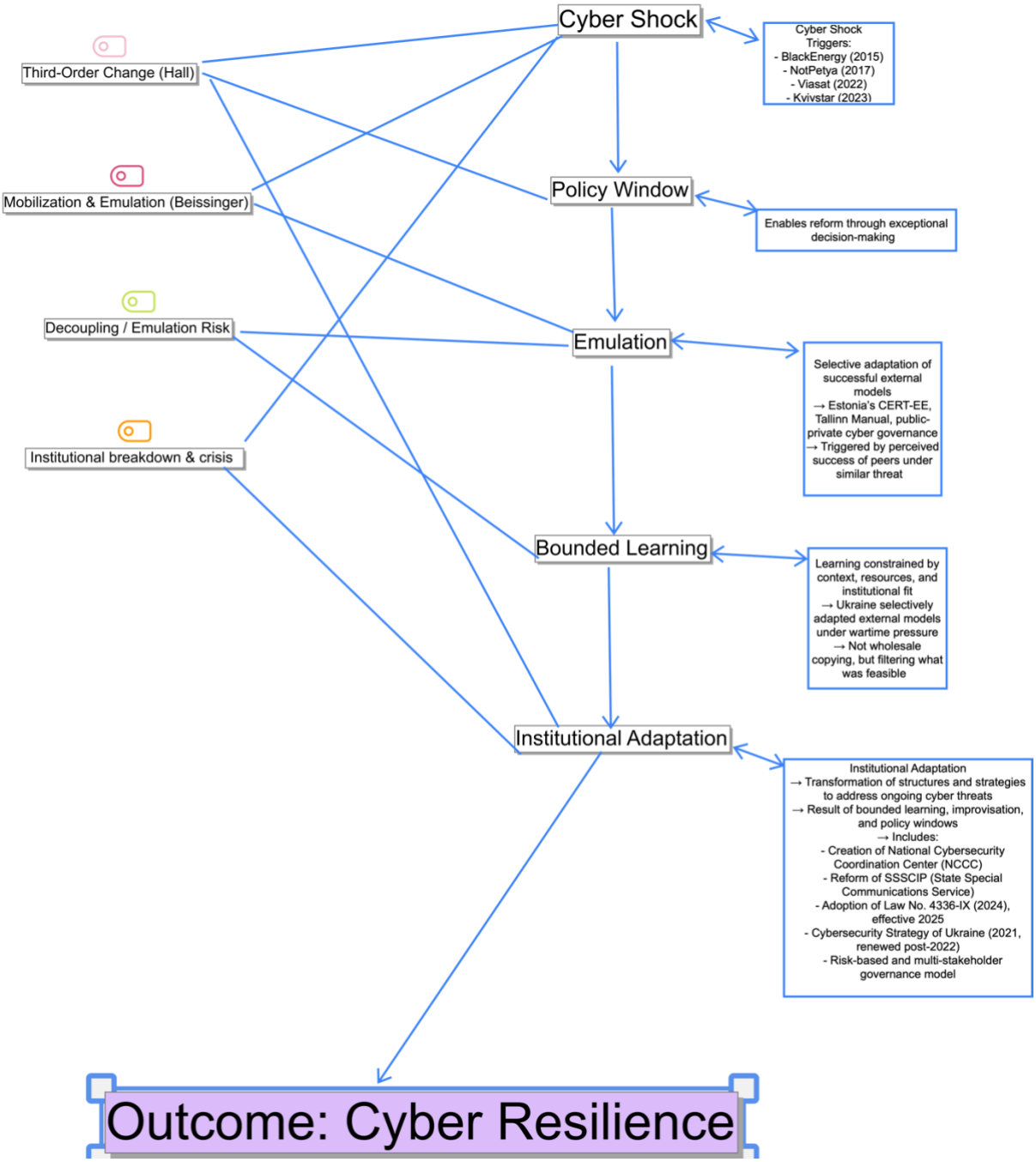

Figure 1. Crisis-Driven Learning: Ukraine's Cyber Resilience [7]

[7] As illustrated in Figure 1, this is not a design or a predicted pattern according to the terms of rationalistic theory. Instead, it is a constantly ongoing process of developing Ukraine's cyber resilience in conditions of constant shocks and during the crisis period of the post-2014 era. The present study employed the MAXQDA programme for the coding and analysis of the primary indicators of the imperial puzzle. The imperial puzzle was defined as the theories of "third-order change" by Hall (1993) and "national mobilisation in times of crisis and shocks" by Beissinger (2002). The latter theory was confirmed by Messenger (2005) through the concept of "imitation of others by a successful example". Examples of the theoretical puzzle were drawn from the conflict rationalistic

Ukraine's pathway to cyber resilience can be conceptualized through a three-stage process: Crisis/Shock → Progression → Development. This model captures how Ukraine's response to cyber aggression was not the result of anticipatory policy design, but rather the product of adaptive learning under pressure.

The first stage, Crisis or Shock (started 2014), refers to major disruptive cyber incidents that served as catalysts for institutional change. Among the most critical were the 2015 BlackEnergy malware attack, which targeted Ukraine's power grid and caused widespread blackouts; the 2017 NotPetya attack, a destructive malware operation that originated in Ukraine and spread globally; and the 2023 cyberattack on Kyivstar, which disabled emergency communications and air raid alert systems during wartime. These events exposed systemic vulnerabilities and made clear that Ukraine's fragmented and outdated cyber infrastructure was inadequate to meet the evolving threat environment.

In response to these shocks, Ukraine entered the second stage: Progression approximately between 2015 and 2021.This period was characterized by reactive measures that gradually evolved into more coordinated institutional efforts. The creation and operational strengthening

theory, which posits that the resilience of Ukraine should be formed by a predicted and constructively developed strategy. The present analysis proposes a dynamic model that commences with cybershocks. In this instance, the cybershocks are considered to be positive policy impacts that have exposed the fragmentation of Ukraine's cybersecurity infrastructure. The model under discussion here identifies key crises – that is, shocks that, as Peter Hall (1993) defined them, can be regarded as 'windows into policy' – thereby enabling third-order changes, not just in instruments, but also in the paradigms of institutional governance itself. The model then demonstrates how Ukrainian actors have responded to these shocks by imitating them. This imitation has had a profound influence on the institutional model, which is based on the Estonian model (for example, CERT-EE, public-private partnerships, the Tallinn Manual principles). However, Ukraine has adapted this imitation selectively, through what has been termed a "non-peaceful" regime, or one that is "under constant fire". This component of the model is a formulation of Mark Beissinge's (2002) concept of mobilisation through observation, as well as the notion of limited imitation proposed by Popovich, Jenne, and Medzyhorski (2020).
The following figure 1 will provide a comprehensive overview of the relevant literature on the subject.
The model also displays a stage of learning, albeit not of direct copying, but of hybrid institutional solutions.
The final result is cyber resilience, which is analysed in more detail in the author's master's thesis. It is defined as a dynamic process caused by shocks and in crisis, not "peacetime", as the model traces this path from initial cyber shocks (for example, the BlackEnergy attacks in 2015 and NotPetya in 2017) to institutional transformation. All diagrams, codebooks, and the original MAXQDA files used for the conceptual model of cyber resilience are available at: https://github.com/BeskaSolomiia/cyberresilience-thesis-maxqda-2025.git

of national cybersecurity institutions marked a turning point. Key actors included the State Service of Special Communications and Information Protection of Ukraine (SSSCIP, 2016) responsible for policy coordination and technical cyber defense; CERT-UA, which transitioned from a nominal entity into an active cyber incident response team with enhanced capabilities; and the Cyber Police (established 2015), tasked with investigating cybercrimes and strengthening public digital safety. During this stage, Ukraine also began articulating a more coherent cyber policy framework through national strategies and legal reforms. Ukraine's cybersecurity policies became embedded in broader national security thinking, supported by updated legislation—such as the Cybersecurity Law of 2017 (No. 2163-VIII) and the Critical Infrastructure Protection Law of 2025 (No. 11290).

The final stage, Development (began to take shape after 2022), reflects a more strategic and integrated approach to cyber resilience. International cooperation with NATO, the EU, and actors like USAID deepened significantly. This stage also saw the transition from purely reactive defense to proactive and even preventive strategies, including Ukraine's growing involvement in cyber diplomacy, joint threat attribution, and participation in EU/NATO cyber exercises. Resilience became institutionalized as both a domestic governance priority and an element of Ukraine's international security identity.

In sum, this three-phase model shows how Ukraine's cyber resilience emerged not from prior design, but through a cumulative process of crisis response, institutional learning, and strategic adaptation to external examples like Estonia.

This model traces how resilience is built over time through learning—not design.

1.6 Research Design and Methods

This thesis employs a longitudinal single-case study of Ukraine between 2014 and 2025. The case selection is justified on both theoretical and empirical grounds. Ukraine represents an extreme case of cyber resilience: despite undergoing sustained cyber aggression, institutional fragmentation, and full-scale war, it managed to develop a functioning and adaptive cybersecurity ecosystem. It also qualifies as a pathway case, offering a valuable opportunity to trace how repeated cyber shocks can generate institutional and strategic learning over time.

Methodologically, the study relies on process tracing to uncover the causal sequences linking cyber shocks to resilience-building. The core analytical logic follows a four-stage model: Cyber shock → Institutional response → Policy learning → Resilience-building.

To operationalize this logic, the empirical analysis is structured around three critical junctures, each corresponding to a major cyberattack that served as a tipping point for policy change and institutional innovation.

These three moments form the basis of three embedded mini-cases within the broader Ukrainian trajectory: the 2015 BlackEnergy attack, which exposed deep vulnerabilities in the national energy grid and prompted the initial mobilization of CERT-UA; the 2017 NotPetya malware campaign, which caused massive public and private sector disruptions and led to the adoption of Ukraine's first Cybersecurity Law (No. 2163-VIII); and the 2023 wartime disruption of Kyivstar services, which paralyzed emergency communications and catalyzed the passage of Law No. 11290 in 2025 aligning Ukraine with EU/NATO cyber resilience frameworks—all of which serve as empirical anchors to test two competing explanations of institutional change: a rationalist model of pre-planned, cost-benefit-driven policymaking, and a learning-based model in which each shock triggered reactive adaptation, bounded emulation, and incremental transformation under crisis conditions (Hall 1993; Beissinger 2002).

These mini-cases are not merely illustrative but serve as causal probes through which I test two competing explanations of policy change: a rationalist model, in which reforms result from anticipatory planning and cost-benefit optimization, and a learning-based model, in which crisis-induced shocks catalyze reactive adaptation, bounded emulation, and institutional transformation over time (Hall 1993; Beissinger 2002).

The expected empirical signatures differ. If the rationalist model holds, one would observe comprehensive preemptive planning, sustained capacity-building in the absence of crises, and cost-benefit deliberation driving policy design. By contrast, if the learning-based model is correct, changes will be clustered around shocks, often improvised, and oriented toward external emulation (particularly of Estonia) rather than endogenous optimization.

Primary sources for this research include both Ukrainian and international documents, such as reports from the *State Service of Special Communications and Information Protection* (SSSCIP)—including *Year in Review: Ukraine's Cyber Defense 2023 and the Statistical Report on Vulnerability Detection and Cyber Incident Response System* (2024); *CERT-UA malware and threat bulletins; the Cyber Police Annual Report* (2024); and key legal and strategic texts including *the 2016 and 2021 Cybersecurity Strategies, Law No. 2163-VIII (2017), and Law No. 11290 (2025)*, as well as international materials such as *Cyber Threat Activity Related to the Russian Invasion of Ukraine (Government of Canada 2022), NATO's Cyber Era: Lessons from Ukraine (2023), Collective Cyber Situational Awareness in the EU (2024), the EU Cyber Resilience Act (2022), and the Ukraine Cyber Chronology (Atlantic Council 2024).*

The analytical strategy involves source triangulation and careful tracing of institutional, legal, and strategic responses across the three critical junctures. The study specifically investigates how Ukraine selectively emulated Estonia's post-2007 cyber reforms—adapting them to its own wartime context through a process of bounded learning rather than direct copying.

1.7 Conclusion and Chapter Outline

This introductory chapter has set the stage for the thesis by presenting the general and specific research questions, theoretical framework, literature review, and methodological approach. I have argued that cyber resilience in Ukraine did not result from anticipatory rational design but emerged incrementally through episodes of crisis-driven learning and bounded emulation. Ukraine's experience challenges conventional assumptions that cyber resilience must be engineered ex ante through cost-benefit planning, and instead suggests that states under hybrid threat can adapt reactively and construct functional resilience over time.

To investigate this claim, I conduct a longitudinal single-case study of Ukraine between 2014 and 2025, structured around three embedded mini-cases that trace policy change after major cyber shocks: the BlackEnergy attack in 2015, the NotPetya campaign in 2017, and the wartime disruption of Kyivstar in 2023. These moments represent critical junctures in which Ukraine transitioned from fragmented response mechanisms to a national cybersecurity architecture with international alignment. In each case, I contrast the predictions of a rationalist model of cyber policy design with a learning-based model of adaptive emulation.

The remainder of this thesis is organized as follows: **Chapter 2** presents the empirical core of the thesis. It reconstructs Ukraine's cyber resilience trajectory through process tracing of the three embedded episodes, drawing on primary documents, government reports, threat bulletins, and legal texts. Each episode is analyzed as a discrete causal case of institutional transformation triggered by cyber disruption. **Chapter 3** steps back from the empirical detail to draw broader theoretical and policy implications. It explores how Ukraine's experience contributes to the general study of cyber resilience, the applicability of bounded learning as a model of crisis adaptation, and the role of emulation in post-Soviet and conflict-affected states. It also reflects on the lessons for NATO, the EU, and future cyber governance regimes.

The **Conclusion** summarizes the findings, revisits the theoretical argument, and outlines avenues for further research. It reinforces the thesis's core claim: that cyber resilience can be forged through crisis, not just designed in anticipation—and that Ukraine offers a model of adaptive resilience under conditions of sustained hybrid war.

Chapter 2: Empirical Case Study on Ukraine's Cyber Resilience

"The term 'electronic Pearl Harbor' metaphorically refers to a surprise cyber-attack of massive destructive potential capable of undermining national security systems."
— Riaz Shad, *Cyber Threat in Interstate Relations* (2018, 101)

When I began investigating how Ukraine developed cyber resilience under conditions of active war, I was struck by a fundamental paradox: How did a state with no pre-existing cyber resilience model manage to construct one while under sustained attack? More specifically, how is resilience actually built when a country lacks the time, institutional capacity, or political consensus for *ex ante* policy design?

These questions guided my empirical investigation. I argue that Ukraine's cyber resilience did not emerge from long-term strategic planning, but rather as a form of social learning under conditions of uncertainty (Hall 1993). As Peter Hall notes, "governments not only 'power'… they also puzzle. Policy-making is a form of collective puzzlement on society's behalf" (Hall 1993, 279). In Ukraine's case, each cyber crisis forced the state to search for answers in real time, reshaping its institutional framework through experience rather than doctrine.

At the same time, this evolution was not purely internal. I draw on Mark Beissinger's (2002) model of *mobilization through observation* to explain how Ukraine selectively emulated successful external models. As Beissinger writes, "within the context of a tide, nationalist movements have greater opportunities to engage in open expression and action… due to the supportive example of others" (Beissinger 2002, 40). Similarly, Ukraine's post-crisis reforms

increasingly mirrored the Estonian approach—demonstrating that policy change was often driven by bounded learning from perceived success stories rather than by clear foresight.

In this chapter, I reconstruct Ukraine's trajectory from institutional fragmentation to strategic coherence by analyzing five major cyber incidents between 2015 and 2024. These cases function as critical junctures, exposing systemic vulnerabilities and opening windows for reactive adaptation. I show that Ukraine's cyber resilience was not born of design but of necessity—mobilized in response to shock, shaped by institutional improvisation, and filtered through the constraints of wartime governance.

2.1 Timeline of Major Cyber Incidents (2014–2024)

This section outlines the major cyberattacks that hit Ukraine between 2014 and 2024. Far from being isolated or random, these incidents constitute a coherent pattern of aggression embedded within Russia's broader hybrid warfare strategy. Each major attack—particularly when it involved critical infrastructure—served as a "critical juncture" that triggered institutional and policy shifts. These events, therefore, form the empirical foundation of my claim that Ukraine's cyber resilience emerged as a product of crisis-driven institutional learning.

The evolution of Ukraine's cybersecurity capacity is best traced through a series of major cyber incidents that served as formative shocks to the national security system. In December 2015, Russian military intelligence operatives, specifically the Sandworm group affiliated with the GRU, executed a coordinated cyberattack against three Ukrainian power companies by compromising SCADA systems. This resulted in a six-hour blackout that affected over 225,000 residents across Ivano-Frankivsk, Chernivtsi, and Kyiv regions, using spear-phishing, malware injection, and remote-access techniques to disable circuit breakers and prevent recovery by operators (European Parliamentary Research Service 2022, 4; Givens et al. 2023, 3).

In June 2017, the NotPetya malware—initially masked as ransomware—was launched against Ukrainian infrastructure via corrupted tax accounting software. It quickly spread globally, causing an estimated $10 billion in damage and crippling sectors such as banking, transportation, and energy, making it one of the most destructive cyberattacks recorded to date (European Parliament 2023, 9; Givens et al. 2023, 6).

As Russian forces prepared for and launched the full-scale invasion in February 2022, a new wave of cyberattacks struck Ukrainian digital infrastructure. The Viasat satellite hack severely disrupted military communications, while destructive wiper malware such as WhisperGate and CaddyWiper targeted government networks in an apparent attempt to paralyze critical state functions at the outset of conventional hostilities (Ukraine Cyber Chronology 2024, 4–6).

In December 2023, the Solntsepek group, again linked to Sandworm, launched a large-scale cyberattack on Kyivstar, Ukraine's largest telecommunications provider. The disruption, which disabled mobile and internet access for 24 million users and affected ATM operations and digital services, was widely characterized as the most significant cyberattack since the war began, illustrating the vulnerability of civilian infrastructure in wartime (Ukraine Cyber Chronology 2024, 8; Givens et al. 2023, 12).

Finally, in early 2024, Ukrainian state registries were subjected to a synchronized cyberattack that temporarily incapacitated essential digital services. While much of the operational detail remains undisclosed, this breach prompted a renewed sense of urgency and contributed to the legislative and institutional push that culminated in the adoption of the 2025 National Cyber Incident Response Framework (European Parliament 2023, 12; Ukraine Cyber Chronology 2024, 10).

These cases are not only indicative of the scale and intent behind Russia's hybrid strategy, but also offer empirical evidence for how Ukraine's institutions responded to cyber threats under wartime conditions. The analysis that follows links each major cyber incident to concrete institutional and legal transformations. Rather than treating the attacks in isolation, I trace how each episode triggered reactive policy change, forming what Peter Hall (1993) describes as a "third-order change" in governance logic. At the same time, I examine how Ukraine's trajectory reflects Mark Beissinger's (2002) model of mobilization through external observation—learning from successful examples like Estonia to inform domestic adaptation.

In this sense, the timeline is not just chronological but causal: each attack marked a critical juncture, forcing a recalibration of Ukraine's cybersecurity paradigm and accelerating the transition from fragmented responses to systemic cyber resilience.

2.2 Ukraine's Cybersecurity Policy Before and After 2014

Before 2014, Ukraine lacked a coherent cybersecurity strategy. The legal foundation was piecemeal: the *Law of Ukraine "On the Fundamentals of National Security of Ukraine*" (2003) briefly mentioned information security; the *Law of Ukraine "On the State Service of Special Communications and Information Protection*" (2006) created a specialized communications security body; and CERT-UA (Computer Emergency Response Team of Ukraine) was formally established in 2007, though with limited operational capacity. As noted in Givens et al. (2023, 2), these measures failed to treat cybersecurity as a distinct strategic field.

Following the 2015 BlackEnergy attack, the *National Security Strategy of Ukraine* was updated to formally recognize cyber threats for the first time (President of Ukraine 2015). This strategic recognition was followed in 2016 by the *first Cybersecurity Strategy of Ukraine*, which laid the conceptual groundwork for a broader legal framework. In 2017, the adoption of *Law No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity in Ukraine"* institutionalized the national cybersecurity system, clearly defining state actors, their roles, and mechanisms of cooperation (Zakon Ukrainy 2017). The *Cybersecurity Strategy was revised in 2021* to reflect evolving threat perceptions, mid-term priorities, and increased institutional maturity (President of Ukraine 2021).

In response to intensified attacks during the full-scale invasion, Ukraine adopted *Law No. 11290 "On Critical Infrastructure Protection"* in 2025, aligning its cyber regime with the EU's *NIS2 Directive*. This legislation introduced a national cyber incident response framework, defined obligations for public-private cooperation, and mandated risk-based protection of critical infrastructure (Zakon Ukrainy 2025).

Taken together, these developments represent a shift from fragmented, reactive policymaking to strategic cybersecurity governance. This evolution is consistent with Peter Hall's

(1993) concept of third-order change—a paradigm shift where not only policy instruments, but also goals and problem definitions are transformed in response to crisis. As Givens et al. observe, Ukraine's policy evolution "was less about preemptive design than about rapid adaptation to escalating hybrid threats" (Givens et al. 2023, 14).

These incidents provide the empirical foundation for understanding cyber resilience as a reactive, iterative, and externally informed process of adaptation. The following section explores how each shock catalyzed shifts in Ukraine's cybersecurity policy and institutional architecture.

2.3 Institutional Evolution: From Fragmented Defense to Coordinated Strategy

Ukraine's cybersecurity institutional architecture evolved significantly in response to repeated shocks, transitioning from a fragmented defense posture to a more coordinated and strategic governance system. This transformation was not linear or preplanned—it unfolded through reactive adaptation, filtered through institutional improvisation and constraint.

The *State Service for Special Communications and Information Protection of Ukraine (SSSCIP)* became the central technical and policy coordinator, overseeing cybersecurity strategy implementation, critical infrastructure protection, and coordination among sectoral actors (Davydiuk and Potii 2024, 14). In 2023 alone, SSSCIP processed over 133 million information security events and documented 1,105 cyber incidents—a 62.5 percent increase from the previous year, reflecting both expanded monitoring capacity and an elevated threat environment (SSSCIP 2023, 6).

CERT-UA, originally created in 2007 with a symbolic mandate, underwent a radical operational expansion. Through international support, especially from USAID, it transformed into a functioning national Computer Emergency Response Team, issuing threat bulletins, responding to incidents, and partnering with both public and private actors (CERT-UA 2023a; CERT-UA 2023b).

The establishment of a Cyber Police Department in 2015 empowered law enforcement to tackle cybercrime, fraud, and disinformation, while also engaging in public outreach and education (Davydiuk and Potii 2024, 19). Parallel developments in the Security Service of Ukraine (SBU) and the Ministry of Defence led to the formation of military cyber defense units—formalizing cyber as an operational military domain.

These shifts were codified through key legislative reforms. *Cybersecurity Law No. 2163-VIII (2017)* defined institutional responsibilities and formalized Ukraine's national

cybersecurity system (Zakon Ukrainy 2017). After the 2022 full-scale invasion, *Law No. 11290 (2025)* introduced a national cyber incident response system, regional response teams, mandatory cyber training, and a risk-based infrastructure protection model, aligning Ukraine with the *EU NIS2 directive* and international standards such as NIST (Zakon Ukrainy 2025; SSSCIP 2023, 11).

As Hall (1993, 279) explains, "Third-order change occurs when the very goals behind policy are reconsidered, involving a shift in the overarching terms of policy discourse." Ukraine's trajectory—from reactive defense to proactive, strategic cyber governance—illustrates precisely such a paradigmatic shift. In this case, institutional mandates were not simply revised; they were reconceptualized in response to existential threat.

At the same time, the evolution of Ukraine's cyber architecture reflects an embedded process of observational learning. As Beissinger (2002, 40) argues in his analysis of mobilization tides, external shocks can generate opportunities "due to the attenuation of institutional constraints and the supportive example of others." In Ukraine's case, the growing pressure of Russian hybrid attacks created both urgency and permission for institutional innovation, enabling reforms that might have been politically impossible under normal conditions. "Today, Ukraine stands on the front line of the most technologically advanced war in the world. In these conditions, the Tallinn Mechanism has become a model of coordinated international support that strengthens our cyber resilience. We highly value this partnership, which helps us respond to threats and build a secure digital environment for Ukraine and the entire democratic world" (Ministry of Foreign Affairs of Ukraine 2025)

Thus, Ukraine's institutional transformation in the cybersecurity sector was neither preordained nor imported wholesale. It was a reactive, layered process—shaped by crisis, sustained by improvisation, and legitimized through adaptation. These developments provide further

empirical support for understanding cyber resilience as an emergent and dynamic response to hybrid warfare, rather than the product of top-down policy design.

Figure 2

The diagram visually confirms this trend: zero funding prior to 2014, cautious increases following cyberattacks, and a sharp rise after 2022—reflecting a pattern of reactive rather than rationalist cybersecurity policy.

Budgetary evidence contradicts the rationalist expectation of ex ante cybersecurity planning**.** Analysis of Ukraine's national budgets from 2010 to 2025 reveals a clear pattern of reactive, not preventive, investment. Prior to 2014, no financial commitments to cybersecurity existed. Strategic planning emerged only after the 2015 BlackEnergy and 2017 NotPetya attacks, with incremental increases in funding and institutional development. The most significant growth occurred post-2022 invasion, culminating in the 2025 adoption of *Law No. 11290.* These shifts were driven by crisis-induced adaptation rather than technocratic

anticipation—undermining rationalist models and supporting theories of reactive, learning-based institutional evolution.[8]

[8] This analysis is based on the full review of the following laws of Ukraine "On the State Budget of Ukraine" for the years 2010–2025:Law of Ukraine "Про Державний бюджет України на 2010 рік" No. 2154-VI of April 27, 2010 (*On the State Budget of Ukraine for 2010*), Law of Ukraine "Про Державний бюджет України на 2011 рік" No. 2857-VI of December 23, 2010 (*...for 2011*), Law of Ukraine "Про Державний бюджет України на 2012 рік" No. 4282-VI of December 22, 2011 (*...for 2012*), Law of Ukraine "Про Державний бюджет України на 2013 рік" No. 5515-VI of December 6, 2012 (*...for 2013*), Law of Ukraine "Про Державний бюджет України на 2014 рік" No. 719-VII of January 16, 2014 (*...for 2014*), Law of Ukraine "Про Державний бюджет України на 2015 рік" No. 80-VIII of December 28, 2014 (*...for 2015*), Law of Ukraine "Про Державний бюджет України на 2016 рік" No. 928-VIII of December 25, 2015 (*...for 2016*), Law of Ukraine "Про Державний бюджет України на 2017 рік" No. 1801-VIII of December 21, 2016 (*...for 2017*),Law of Ukraine "Про Державний бюджет України на 2018 рік" No. 2246-VIII of December 7, 2017 (*...for 2018*), Law of Ukraine "Про Державний бюджет України на 2019 рік" No. 2629-VIII of November 23, 2018 (*...for 2019*), Law of Ukraine "Про Державний бюджет України на 2020 рік" No. 294-IX of November 14, 2019 (*...for 2020*), Law of Ukraine "Про Державний бюджет України на 2021 рік" No. 1082-IX of December 15, 2020 (*...for 2021*), Law of Ukraine "Про Державний бюджет України на 2022 рік" No. 1928-IX of December 2, 2021 (*...for 2022*), Law of Ukraine "Про Державний бюджет України на 2023 рік" No. 2710-IX of November 3, 2022 (*...for 2023*), Law of Ukraine "Про Державний бюджет України на 2024 рік" No. 3460-IX of November 9, 2023 (*...for 2024*), Law of Ukraine "Про Державний бюджет України на 2025 рік" No. 4059-IX of November 19, 2024 (*...for 2025*). (All Laws are my own translation

2.4 Estonia as a Model of Success-Driven and Bounded Learning

In line with my theoretical framework that combines Peter Hall's (1993) concept of third-order policy change and Mark Beissinger's (2002) model of mobilization through external observation, this section shows this Estonia served as a referential model for understanding how Ukraine developed cyber resilience under conditions of war. Estonia's transformation after the 2007 cyberattacks provided Ukraine with an example of how institutional capacity could be rebuilt in the wake of systemic digital disruption. Analyzing Estonia's national cybersecurity strategy for 2019-2022, we clearly see that the most important goals are cooperation and creating a foundation for the development of less developed countries, namely "We will promote competitive and sustainable cyber capability in partner countries, disseminating Estonia's experience to third countries through the EU and international projects." (Ministry of Economic Affairs and Communications of Estonia [MKM] 2019, 18)

As Beissinger notes, "within the context of a tide, nationalist movements have greater opportunities to engage in open expression and action… due to the supportive example of others" (Beissinger 2002, 40). Strategic learning, I argue, follows the same dynamic: pressure and uncertainty create openings for emulation based on visible success.

Ukraine's cybersecurity learning from Estonia reflects this logic of bounded, success-driven adaptation. CERT-EE, Estonia's national Computer Emergency Response Team, was established in 2006 under the Information System Authority (RIA). It was one of the first state-level institutions in Europe to be empowered with both technical response capacity and national coordination functions.[9] Following the 2007 cyberattacks, CERT-EE became a cornerstone of Estonia's cyber resilience model—supporting cross-sectoral response, public-private cooperation, and integration into NATO and EU cyber frameworks.[10] This structure later served

[10] Estonian Information System Authority. "About CERT-EE." *CERT-EE Official Website*. Accessed May 18, 2025. https://www.ria.ee/en/search?search_term=about+CERT+EE&type=News&sort_by=created

as an informal reference point for the evolution of Ukraine's CERT-UA after 2016. CERT-UA[11] was established in 2007, shortly after CERT-EE, though for years it remained underfunded and operationally weak. Institutional change accelerated after 2016, when Ukraine began building a coherent cyber governance architecture. The Tallinn Manual on the international law of cyber operations, though not legally binding, influenced Ukraine's doctrinal discourse and strategic planning (Schmitt 2013). In both cases, national cyber strategies emerged in response to digital crises—but the nature of the crises, and the institutional conditions under which they occurred, differed sharply. "Ukraine is grateful to Estonia for its assistance not only in enhancing national cyber resilience, but also for its willingness to share its experience in creating the most convenient digital state. Based on the Estonian X-Road, we developed Trembita, a system for exchanging information between registries, which became the foundation for the Diia ecosystem" (Ministry of Foreign Affairs of Ukraine 2024).[12]

As Meseguer (2005) and Popovic, Jenne, and Medzihorsky (2020) argue, emulation is never unbounded. Rather than simple duplication, policy learning is shaped by domestic conditions, resource constraints, and symbolic pressures. As the latter authors explain, "policy models that perform well in one context can only be partially transplanted into another" due to differences in structure, incentives, and timing (Popovic, Jenne, and Medzihorsky 2020, 1453). Ukraine's pre-2014 cybersecurity landscape was fragmented and reactive. Under conditions of full-scale war after 2022, the government had to improvise, adapting foreign models under severe

[11] CERT-UA. "Official Website of the Computer Emergency Response Team of Ukraine." Accessed May 18, 2025. https://cert.gov.ua.

[12] In order to demonstrate that Ukraine's cyber resilience reforms involved a bounded learning process inspired by Estonia (rather than merely coinciding with NATO or EU pressures), I systematically analyzed a curated set of primary sources, including national strategies, cyber incident reports, international policy briefings, and legal frameworks.To do this, I used a two-layered coding strategy in MAXQDA-Lexical tracing and Theoretical coding and I'm actually integrating that into the qualitative part—especially how it's emphasized in the speeches and statements by key leaders at the time.
This method, I believe, provides empirical grounding to your question: *How do you know the timing isn't just a coincidence or driven top-down by NATO/EU?* The textual evidence shows that Ukrainian reforms—especially the development of CERT-UA, references to CCDCOE, and the framing of Estonia as a "cyber benchmark"—were articulated in ways that suggest bottom-up emulation based on observed success, not only external pressure. (The table is attached in the appendix)

constraints. This aligns with their argument that "emulation is particularly likely when the state's goals are unclear… or when the environment creates symbolic uncertainty" (Popovic, Jenne, and Medzihorsky 2020, 1453).

This logic of bounded learning also fits Peter Hall's theory of third-order change, where "the very goals behind policy are reconsidered, involving a shift in the overarching terms of policy discourse" (Hall 1993, 279). Ukraine's cyber policy transformed from a technical subfield to a pillar of national security, driven less by doctrine than by the necessity of survival. Importantly, this learning was not only institutional but societal. Estonia's Cyber Defence League—a volunteer force embedded in national defense—served as inspiration for Ukraine's IT Army, which mobilized civilian actors to conduct cyber operations during wartime. Although Ukraine's version was informal and unregulated, the underlying logic of defensive civic engagement echoed the Estonian approach.

However, the Ukrainian context added a new layer to the emulation dynamic. As Kostyuk and Zhukov (2017) point out, "most research has focused on the consequences of cyber attacks for peacetime deterrence rather than wartime compellence" (318). In other words, Ukraine was not learning how to prevent attacks in the abstract—it was learning how to survive under continuous digital siege. As they further argue, "although kinetic operations explain the timing of other kinetic operations, low-level cyber attacks have no discernible effect on violence in the physical world" (Kostyuk and Zhukov 2017, 340). This underscores the fact that cyber resilience in wartime functions on a different logic from peacetime deterrence—it is iterative, adaptive, and oriented toward institutional continuity rather than escalation avoidance.

In sum, Estonia acted as a referential anchor: a source of legitimacy and inspiration, but not a blueprint. Ukraine's institutional learning was strategic but also improvised, shaped by the

trauma of war and the urgency of reform. This was not simple policy diffusion. It was resilience by necessity—filtered, adapted, and translated through crisis.

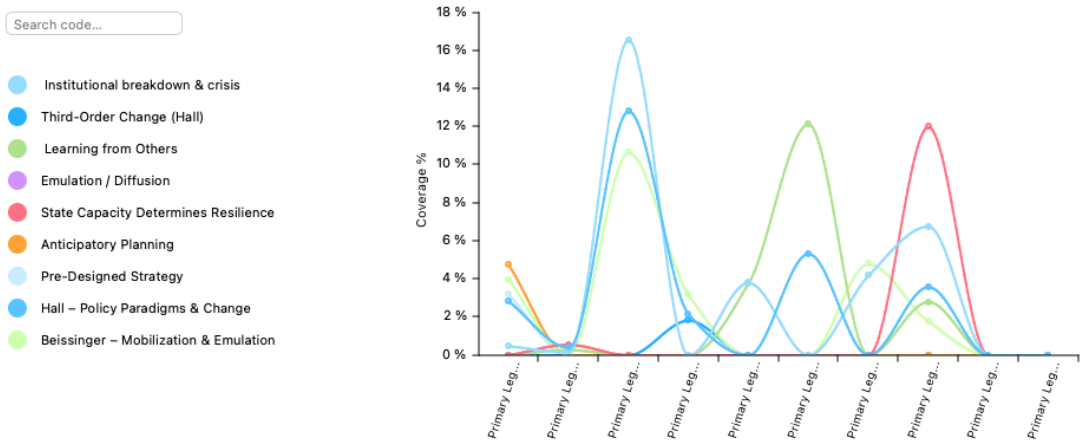

Figure 3 Code Coverage Across Primary Legal and Policy Documents [13]

[13] In this figure, I have created a coding overview using MAXQDA to check how my empirical puzzle and theories are implemented in primary sources relevant to my master's thesis. This image shows how codes from Peter Hall's "third-order theory" of change and Mark Basinger's successful "imitation model", as well as other options (proactive planning, pre-developed strategies, state capacity), can be seen in important Ukrainian legal and strategic documents and reports from the EU and key organisations in cyberspace. The database includes laws, cybersecurity strategies, reports and information from state organisations such as SSSCIP and the National Security and Defence Council. The figure is based on a comparative coding of the following key documents: *Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" No. 2163-VIII, October 5, 2017. National Cybersecurity Strategy of Ukraine (2021), enacted by Presidential Decree No. 96/2021. Draft Information Security Concept of Ukraine (2023). Law of Ukraine "On the Fundamentals of National Security of Ukraine," July 22, 2003. Cyber Digest, May 2023 – State Service for Special Communications and Information Protection of Ukraine. Cyber Incident Response Report, State Cyber Protection Centre, 2023. "Cyber Considerations from the Conflict in Ukraine," Center for Strategic and International Studies (CSIS), 2022. "Book of Law: Cybersecurity and International Legal Frameworks," Ukrainian Institute for the Future, 2023. European Parliamentary Research Service. 2022. "Cybersecurity in Ukraine: State of Play and Future Challenges."*
Thales Group. 2023. "Cyber Conflict in Ukraine: Analysis of Russian Tactics and Ukrainian Resilience."
This mapping aimed to track which theoretical explanations were most frequently reflected in Ukraine's response to cyber threats during the war. The documents were chosen because they are relevant to the changes in Ukraine's cybersecurity, and the information in them was coded line by line using categories developed through deductive reasoning.
The resulting visualisation supports the idea that Ukraine's digital resilience is not more likely to be affected by rational theories, designs and planning. Instead, it has developed through limited learning, institutional improvisation and strategic copying of examples such as Estonia. The image illustrates how cyber resilience, as demonstrated in wartime Ukraine, is a combination of swift institutional adjustments and adapting to pressure.

Chapter 3: Broader Implications for Cyber Resilience and International Security

Ukraine's experience with cyber resilience offers crucial insights into how states can adapt their digital security strategies under conditions of prolonged hybrid aggression. Rather than presenting a linear trajectory of cyber preparedness, Ukraine's model reflects a dynamic, crisis-driven, and externally informed process that reshapes traditional understandings of cyber governance. This final chapter explores how Ukraine's resilience-building contributes to the evolving doctrines of NATO, the EU, and the broader international legal community, offering lessons for conflict-affected states and global security institutions.

First, Estonia's model must be reassessed not as a blueprint, but as a referential anchor—a flexible governance framework that Ukraine selectively emulated. As Chapter 2 demonstrated, Ukraine's learning process was bounded by wartime constraints but inspired by Estonia's strategic foresight and institutional coherence. This selective emulation confirms the central premise of Beissinger's (2002) mobilization theory: external examples matter not because they are perfectly replicable, but because they provide legitimacy, structure, and symbolic clarity during times of uncertainty. In the cyber domain, Estonia exemplified resilience as a governance principle; Ukraine transformed that principle into a survival strategy.

Ukraine's evolving cybersecurity posture has begun to influence NATO and EU cyber doctrines. This influence is visible in three domains: strategic alignment, legal harmonization, and the integration of hybrid civilian-military cyber capabilities. Ukraine's adaptation of the EU's NIS2 Directive and the 2025 Critical Infrastructure Protection Law reflects an alignment with Euro-Atlantic resilience standards. Similarly, participation in NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and joint cyber exercises highlights the practical convergence of Ukraine's defensive posture with alliance norms. As the European Parliament

noted in its 2024 briefing, Ukraine's war-driven cyber evolution has made it "a laboratory for NATO's future cyber defence priorities" (European Parliamentary Research Service 2024, 18).

This feedback loop—where Ukraine absorbs and then reshapes institutional norms—illustrates what the EU now terms "reverse conditionality" in resilience-building. Rather than simply internalizing Western norms, Ukraine is contributing to their redefinition. Its operational experience has exposed gaps in EU/NATO response coordination, crisis management, and attribution protocols. In particular, the IT Army model—however controversial—demonstrates the viability of decentralized civic mobilization in cyberspace. The integration of public volunteers into a state-sanctioned (though loosely regulated) cyber defense structure is now being studied as a resilience multiplier, particularly in small or vulnerable states lacking conventional cyber capacity (NATO StratCom COE 2023, 22).

As Popovic, Jenne, and Medzihorsky explain, "rather than creating policies from scratch, governments search for general policy models that have a record of success in similar states, anticipating that these models will yield similar material benefits to the adoptee" (Popovic, Jenne, and Medzihorsky 2020, 1452). Ukraine's process of institutional adaptation closely follows this logic of success-driven emulation, filtered through its unique wartime constraints.

This redefinition of cyber resilience carries legal implications as well. As the Tallinn Manual and UN OEWG processes suggest, states are expected to maintain due diligence, protect critical infrastructure, and uphold responsible behavior in cyberspace. Ukraine's improvisational reforms challenge the assumption that such obligations must always derive from peacetime stability. Instead, it illustrates that resilience can be forged in wartime through necessity-driven adaptation, even when attribution remains murky and strategic ambiguity is a persistent feature of conflict (Schmitt 2017).

This perspective has broader implications for cyber governance in fragile or threatened states. Rather than assuming that cyber resilience is a luxury of developed democracies, Ukraine's case shows that resilience can emerge in hostile environments. As Kostyuk and Zhukov (2017) argue, "most research has focused on the consequences of cyber attacks for peacetime deterrence rather than wartime compellence" (318). Ukraine reverses this logic. Its transformation was not engineered in the abstract but forged in the crucible of conflict. This supports Hall's (1993) theory of third-order change: resilience was not merely a shift in policy tools, but in governing paradigms.

Moreover, Ukraine's trajectory complicates traditional assumptions about cyber warfare. If, as Kostyuk and Zhukov also note, "low-level cyber attacks have no discernible effect on violence in the physical world" (2017, 340), then the strategic value of cyber resilience lies less in deterring violence and more in preserving institutional continuity. Ukraine's ability to restore services, maintain public communication, and secure critical data amid disruption reveals a form of governance that is not deterrence-centric, but adaptation-centric.

Finally, Ukraine's cyber resilience illustrates a key lesson for international security regimes: resilience is not the endpoint of stability, but the mechanism for surviving instability. In this sense, Ukraine serves not as an exception, but as a precedent. It demonstrates how resilience can be constructed through iterative adaptation, selective emulation, and decentralized mobilization. For NATO, the EU, and the UN, this means rethinking resilience as an operational imperative, not just a normative goal. For conflict-affected states, it signals that cyber resilience is attainable not in spite of crisis, but through it.

Conclusion

This thesis set out to answer a deceptively simple yet urgent question: how does a state build cyber resilience under conditions of sustained cyber aggression, rather than in times of stability and foresight? Drawing on the longitudinal case of Ukraine, the study has demonstrated that cyber resilience does not emerge from rationalist design or pre-emptive planning. Instead, it is forged through disruption, pressure, and adaptation. Ukraine's experience illustrates that resilience is not a static attribute, but a dynamic process driven by institutional learning, strategic adaptation, and bounded emulation of external models.

Ukraine's cyber trajectory since 2014 provides a "least likely" case for the development of resilience. It began with fragmented legal frameworks, minimal anticipatory capacity, and limited international coordination. Yet, in the wake of successive shocks—from the 2015 BlackEnergy attack, through the 2017 NotPetya malware, to the 2023 Kyivstar breach—Ukraine incrementally transformed its cyber governance structure. These crises acted as critical junctures, opening windows for institutional improvisation and legal reform. Across each episode, Ukraine responded not by following pre-determined protocols but by learning from experience, absorbing lessons, and selectively emulating Estonia's model within wartime constraints.

Theoretically, the thesis has reconceptualized cyber resilience as a product of "learning under fire." Using Peter Hall's (1993) theory of third-order policy change and Mark Beissinger's (2002) model of mobilization through emulation, it developed a learning-based model of cyber resilience. This model frames resilience not as a end state but as an emergent capacity—built through shocks, recalibrations, and institutional memory. Empirically, the Ukrainian case challenges dominant assumptions that cyber resilience is a function of ex ante planning and capacity. Instead, it shows that resilience can develop reactively, even under structural fragility, when institutions are compelled to adapt.

Practically, the findings hold relevance for conflict-affected and transitioning states facing cyber threats without strong institutional foundations. Ukraine demonstrates that cyber resilience can be cultivated through strategic coordination, legal harmonization, and civic mobilization—even in the absence of perfect defense. For international organizations such as NATO and the EU, the Ukrainian case signals the importance of supporting not only cyber defense capacities but also adaptive governance, legal interoperability, and whole-of-society resilience.

This thesis has also contributed to bridging the gap between legal and political understandings of resilience. Cyber resilience, as shown here, is not simply a technical fix or an operational strategy—it is a normative commitment to governance amid uncertainty. As hybrid warfare blurs the boundaries between war and peace, digital and physical, civilian and military, resilience becomes the condition for continuity. Ukraine's story is not a cyber anomaly—it is a preview of how states will have to govern through disruption in the twenty-first century.

References

Andrews, Julian. 2020. *Cyberwarfare: Security, Strategy and Conflict in the Information Age*. London: Routledge.

Barnea, Hadar, Amit Weiss, and Eyal Shemer. 2020. "Resilience in the Age of Cyber Threats: Multidimensional State Capacities." *Journal of Cybersecurity Studies* 5 (2): 67–89.

Beissinger, Mark R. 2002. *Nationalist Mobilization and the Collapse of the Soviet State*. Cambridge: Cambridge University Press.

Bendiek, Annegret, and Roderick Maat. 2021. "The EU's Cybersecurity Strategy: A Foreign Policy Perspective." SWP Research Paper 4. Berlin: German Institute for International and Security Affairs.

Berkes, Fikret, and Helen Ross. 2013. "Community Resilience: Toward an Integrated Approach." *Society & Natural Resources* 26 (1): 5–20.

Carr, Madeline. 2016. *US Power and the Internet in International Relations*. London: Palgrave Macmillan.

CERT-UA. 2023. *Annual Report on Cyber Incidents in Ukraine*. Kyiv: State Service of Special Communications and Information Protection of Ukraine.

CERT-UA. 2024. *Cyber Threat Landscape in Ukraine 2024*. Kyiv: SSSCIP.

Chiara, Maria, and Elisabetta Brighi. 2024. "Hybrid Threats and the Law: Sovereignty in the Age of Digital Conflict." *European Security Review* 32 (1): 55–72.

Council of Europe. *Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols*. Opened for signature in Budapest, November 23, 2001.

Davydiuk, Oleh, and Viktor Potii. 2024. *Cybersecurity in Ukraine: National Overview 2023*. Kyiv: SSSCIP.

De Mauro, Andrea, Marco Greco, and Michele Grimaldi. 2018. "A Formal Definition of Big Data Based on Its Essential Features." *Library Review* 65 (3): 122–135.

Dobbin, Frank, Beth Simmons, and Geoffrey Garrett. 2007. "The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning?" *Annual Review of Sociology* 33: 449–472.

Dunn Cavelty, Myriam. 2018. "Cybersecurity and Resilience as Strategic Narratives." *European Review of International Studies* 5 (3): 6–23.

Dunn Cavelty, Myriam, and Andreas Wenger. 2023. *Cybersecurity in Practice: Theory and Policy for Resilience*. London: Routledge.

Eichensehr, Kristen E. 2022. "Ukraine, Cyberattacks, and the Lessons for International Law." *AJIL Unbound* 116: 65–69.

ENISA. 2022. *ENISA Threat Landscape 2022*.

European Commission. 2022. *Cyber Resilience Act Proposal*. Brussels.

European Parliamentary Research Service. 2022. *Cybersecurity in the EU: State of Play and Outlook for 2023*. Brussels.

European Parliament. 2023. *Briefing on the Cyber Threat Landscape in Europe*. Brussels.

Fearon, James D. 1995. "Rationalist Explanations for War." *International Organization* 49 (3): 379–414.

Fotescu, Iulian, Elena Dumitrescu, Robert Negoiță, and George Măzăreanu. 2021. "NATO Cyber Defence Policy Evolution." *Journal of Strategic and Security Studies* 14 (3): 105–120.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41–73.

Givens, Austin, Kimberly Zenz, and Taras Kuzio. 2023. *Cyberwarfare in Ukraine: Lessons for the Future*. Washington, DC: Atlantic Council.

Gilardi, Fabrizio, Katharina Füglister, and Stéphane Luyet. 2009. "Learning from Others: The Diffusion of Hospital Financing Reforms in OECD Countries." *Comparative Political Studies* 42 (4): 549–573.

Hall, Peter A. 1993. "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain." *Comparative Politics* 25 (3): 275–296.

Herzog, Stephen. 2017. "Revisiting the Estonian Cyberattacks: Digital Threats and Multinational Responses." *Journal of Strategic Studies* 40 (5): 638–662.

ICRC. 2020. *International Humanitarian Law and Cyber Operations during Armed Conflicts*. Geneva: International Committee of the Red Cross.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2017. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 61 (5): 975–1000.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation.

Meseguer, Covadonga. 2005. "Policy Learning, Policy Diffusion, and the Making of a New Order." *The Annals of the American Academy of Political and Social Science* 598 (1): 67–82.

Milanova, Nina. 2020. "Cyber Resilience as a Regulatory Paradigm in the EU." *Journal of Information Law* 6 (2): 113–127.

Milanova, Nadja. 2020. "Institutional Resilience and Building Integrity in the Defense and Security Sector." *Connections: The Quarterly Journal* 19 (3): 67–75.

Ministry of Economic Affairs and Communications of Estonia (MKM). 2019. *2019–2022 Cybersecurity Strategy.* Tallinn: MKM. Majandus-ja Kommunikatsiooniministeerium, "2019-2022 Cybersecurity Strategy", *Majandus-ja Kommunikatsiooniministeerium,* 2019.

Ministry of Foreign Affairs of Ukraine. 2024. "Ukraine–Estonia Cyber Partnership: Trembita and the Diia Ecosystem." Ministry of Foreign Affairs of Ukraine, April 2024.

Ministry of Foreign Affairs of Ukraine. 2025. *Ukraine's Cyber Diplomacy Strategy*. Kyiv: MFA of Ukraine.

Ministry of Foreign Affairs of Ukraine. 2025. *Statement at the Tallinn Mechanism Coordination Group Meeting*. Kyiv: MFA of Ukraine.

Microsoft. 2023. *Defending Ukraine: Early Lessons from the Cyber War*. Redmond, WA: Microsoft Security Team.

Munusamy, Samuel, and Mansour Khodadadi. 2023. "Cyber Resilience in Practice: An Integrated Framework." *Cyber Policy Journal* 8 (1): 32–47.

NATO. 2021. *NATO's Cyber Defence Policy and Strategic Concept*. Brussels.

NATO. *Strengthened Resilience Commitment*. Adopted June 14, 2021. Last updated September 15, 2022.

NATO StratCom COE. 2023. *Civic Cyber Defence: Lessons from the IT Army of Ukraine*. Riga.

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris.

OEWG. 2021. *Final Report of the Open-Ended Working Group on Developments in the Field of ICT in the Context of International Security*. United Nations.

Ottis, Rain. 2008. "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective." *Proceedings of the 7th European Conference on Information Warfare*.

Panetta, Leon E. 2012. *"Defending the Nation from Cyber Attack."* Speech delivered at Business Executives for National Security, New York, NY, October 11, 2012. U.S. Department of Defense.

Papakonstantinou, Vagelis. 2022. "The IT Army of Ukraine and Civic Cyber Engagement." *Computer Law & Security Review* 46: 105738.

Perez, Luis, Sebastian Bocanet, and Davide Sallos. 2024. "Resilience in Crisis: Organizational Learning and Cyber Readiness." *Global Policy Review* 9 (2): 112–128.

Popovic, Milos, Erin K. Jenne, and Juraj Medzihorsky. 2020. "Authoritarian Emulation: The Adoption of Repressive Strategies in Competitive Authoritarian Regimes." *Comparative Political Studies* 53 (9): 1445–1479.

President of Ukraine. 2015. *National Security Strategy of Ukraine*. Decree No. 287/2015. President of Ukraine. 2021. *Cybersecurity Strategy of Ukraine*. Decree No. 96/2021.

Rahman, Habib, and Richard Cachia. 2021. *Building Cyber Resilience in Europe*. Brussels: European Parliament.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. London: Hurst.

Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Shaffique, Zara. 2024. "The EU Cyber Resilience Act: From Security by Design to Legal Accountability." *European Journal of Law and Technology* 15 (1): 1–19.

Shaw, Michael, Lena Wulff, and Jonah Ellison. 2022. "Embedding Resilience into National Cyber Infrastructures." *Cybersecurity Policy Review* 11 (2): 44–60.

Shad, Riaz. 2018. *Cyber Threat in Interstate Relations*. Islamabad: National Defence University Press.

Štitilis, Darius, Vita Malinauskaitė, and Paulius Pakutinskas. 2017. "Cybersecurity Legal Regulation and the Problems of Critical Infrastructure Protection." *Baltic Journal of Law & Politics* 10 (1): 71–92.

SSSCIP. 2023. *Ukraine's Cyber Defence: Year in Review*. Kyiv: State Service of Special Communications and Information Protection of Ukraine.

SSSCIP. 2024. *Statistical Report on Cyber Vulnerability Detection and Incident Response*. Kyiv.

Thales Group. *Extended Report: Cyber Conflict in Ukraine*. April 5, 2023.

Tasheva, Alyona. 2021. "Cyber Sovereignty and the Fight for Ukraine's Digital Future." *Foreign Policy Centre Briefing*.

Tiirmaa-Klaar, Heli. 2024. *Strategic Cybersecurity Governance: Lessons from Estonia*. London: Routledge.

Topor, Eugenia. 2024. "Sovereignty in Cyberspace: Hybrid Warfare and Resilience in Ukraine." *Global Affairs Review* 6 (1): 55–74.

Ukraine Cyber Chronology. 2024. *Cyber Incidents Timeline (2014–2024)*. Washington: Atlantic Council.

Zakon Ukrainy. 2017. *Pro osnovni zasady zabezpechennya kiberbezpeky Ukrainy* [Law on the Basic Principles of Ensuring Cybersecurity in Ukraine]. Law No. 2163-VIII.

Zakon Ukrainy. 2025. *Pro zakhyst krytychnoi infrastruktury* [Law on the Protection of Critical Infrastructure]. Law No. 11290.

Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023–2024* (Ottawa: Communications Security Establishment, 2023), 13,

APPENDIX

Code Matrix Browser

	Institutional breakdown & crisis	Third-Order Change (Hall)	Learning from Others	Emulation / Diffusion	State Capacity Determines Resilience	Anticipatory Planning	Pre-Designe Strategy
Estonia case _primary Sourses and speeches	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
Primary Legal and Strategic Documents	3,70%	0,41%	2,47%	0,00%	2,88%	0,41%	0,21%
Empirical/conflict-specific sources	0,00%	0,00%	2,06%	1,03%	3,29%	2,88%	2,88%
Theoretical sources	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%

The relation matrix below visualizes the intersection between theoretical and empirical codes in my case study analys
institutional emulation from Estonia ('Learning from Estonia – empirical evidence') intersects with Beissinger's theore
overlapping segments indicate instances where Ukrainian cybersecurity reforms were not only temporally linked to E
aligned, thus substantiating the theory with process-tracing evidence. This directly addresses the critique regarding c
agency and selective institutional learning.

Learning from Estonia – empirical evidence

Created: Solomiia Beska, 27.05.25 10:42 Modified: Solomiia Beska, 27.05.25 15:28

This theoretical code is supported empirically by the code ‘Learning from Estonia – empirical evidence’, which includes all identified moments where Ukrainian actors adapt Estonian cybersecurity structures post-2007

Empirical sources were used to test the learning-by-emulation hypothesis.

To test the theory that Ukraine’s cyber resilience model developed through a limited learning process based on the “successful example” of Estonia, an analysis of primary sources published between 2019 and 2025 was conducted. These documents included official statements, strategic documents and public records from Ukrainian and Estonian government agencies, as well as the work of the Tallinn Mechanism and the CCDCOE Steering Committee.

The following documents were selected and coded using the Beissinger theoretical code, 'Mobilisation and Emulation', and its empirical subcode, 'Learning from Estonia' – empirical evidence.

Ministry of Foreign Affairs of Ukraine (2024–2025): A series of official communications highlighting recurring bilateral cyber cooperation initiatives with Estonia, including the Ukrainian-Estonian Business Forum (2024), meetings of the Tallinn Mechanism Coordination Group (2025) and Ukrainian participation in cyber diplomacy at the Second Global Conference on Cyber Capacity Building (2025).

Tallinn Mechanism (2024): A collective statement by participating states recognising Ukraine’s role in implementing cyber resilience under pressure, and Estonia’s contribution as a reference partner.

Ministry of Economic Affairs and Communications of Estonia (2022): The Estonian National Cybersecurity Strategy (2019–2022) outlines the institutional structures (e.g. CERT-EE and the Cyber Defence League) that have served as models for Ukraine's adaptation.

SSSCIP and eGA (2024): Joint announcements on enhancing the resilience of critical infrastructure in Ukraine using frameworks developed by the Estonian eGovernment Academy (eGA), confirming the transfer and adaptation of experience.

The National Cybersecurity Strategy of Ukraine (2021) and the NSDC documents (2025) These documents provide contextual evidence that Ukraine’s strategic policies are increasingly influenced by Estonian approaches, such as risk-based management and multi-stakeholder coordination.

https://github.com/BeskaSolomiia/cyberresilience-thesis-maxqda-2025.git